??????????? ?? ???????????? ????????? ??????? ???????? ?? Windows ? Kaspersky Industrial CyberSecurity for Nodes 4.5

????????

??????? ??????? Windows — ???? ?? ????? ?????? ????????? ?????? ??? ??????????? ???? ? ????????????? ??????????. ?????? ???????? ? ??????? — ?? ????? ???????????? ?? ????????? ??????? ???????????? — ????????? ???? ? ???? ??????? ? ??????????? ???????????????? (Event ID). ?????? ????? ??????? ?? ???????????? ???? ????? ???? ????????, ? ?????? ??????????? ?? ????????????? ???????????? — ????????? ????????? ???, ????? ??????? ???????? ??????????? ????????, ?? ?????? ? ????????????? ????.

????????? **?????? ????????** ? Kaspersky Industrial CyberSecurity for Nodes 4.5 ???????????? ????????? ????????? ??? ??????? ???? ??????. ? ???? ?????? ?? ????????, ??? ????????? ????????? ???? ?????????, ?? ????? ??????? ?? Windows ???????? ???????? ? ?????? ??????? ? ??? ???????????????? ?? ???????????????? ??? ????????? ????.

---

1. ??? ????? «?????? ????????» ? KICS for Nodes 4.5

????????? **?????? ????????** ???????????? ???????????? ????????? ????? ?? ?????? ???????? ??????? Windows. ??? ???????????? ????????? ???????????? ????????? ? ??????? ????????? ???????????? ????????????????, ??? ??? ??? ????????? ????? ????????? ?? ??????? ?????????.

KICS for Nodes ???????????? ??????? ??????? Windows ? ???????? ????????? ? ???????????? ? ????????? ???? ?????:

- **???????????????? ???????** — ????????? ????????????? ?????? ??? ???????????? ????????.

- **?????????????? ??????** — ????????? ?????? ?????????? ???????? ??????????? ?? ?????? ????????????? ??????? (Event ID) ? ????????? ????????.

??? ??????????? ?????? ??????? ????????? ??????? ??????? ?? ???????? **« ???????????»**, ??? ??????????? ?????? ????????? ????? ? ????? ?????? ???????.

---

2. ?????????????? ???????: ??? ????????????? ?? ?????????

? KICS for Nodes 4.5 ???????? **???? ?????????????? ??????**. ?? ?????? ???????, ?? ????? ????????, ????????? ? ?????????? ????????? ????????.

Правило	Что обнаруживает
?????????? ????????? ??????? ?????? ?????? ? ??????? ???????	??????????? ????????? ??????? ????? (???????, ?????? ??????)
?????????? ????????????? ?????????? ?? ????? ???????? ?????? ?????	????? ? ????????? ????? ??? ? ????????? ???????
?????????? ???????? ???????????? ???????? Windows	??????? ??? ????????? ???????? ??????
?????????? ????????????? ?????????? ?? ??????? ????? ???????????? ??????	????????? ????? ????? — ??????? ?????????? ??????? (persistence)
?????????? ????????????? ????????????? ? ????? ????????? ??????? ??????	???????????? ????? ??????? ?????? (???????, ? ????????)
?????????? ???????? ????? Kerberos forged PAC (MS14-068)	??????? ????????? ?????????? ????? ?????????? Kerberos

Правило	Что обнаруживает
?????????? ????????????? ????????? ???????????????? ?????? ?????????????	???????????????? ?????????? ????????????? ? ?????? Administrators

???????? ????????????? ?????????

??? ??????? «?????????? ????????? ??????? ?????? ?????? ? ??????? ???????» ????? ??????:

- **?????????? ???????** (?? ????????? — 10)
- **?????????? ???????** (?? ????????? — 300 ??????)

??? ????????? ???????????? ??????? ??? ?????????? ?????: ????????, ??? ???????? ? ??????? ????????????? ????????? ?????? ????? ????????? ?????, ????? ??????? ????? ?????? ????????????.

??? ??????? «?????????? ????????????? ?????????? ?? ????? ???????? ?????? ?????» ?????:

- ?????? **????????? ????????**, ? ??????? ???????? ??? ??????? ????? ????????? ??????????? (????????, ? 00:00 ?? 06:00)
- ???????????? **?????? ?????????? ????????????? ? IP-???????** (IPv4 ? IPv6), ??? ??????? ??????? ?? ???????????

---

3. ???????????????? ???????: ???????? ??? ???? ??????

???? ???????????????? ?????? ????????????, ?? ?????? **???????? ??????????? ???????** ?? ?????? ?????????? Event ID.

??? ???????? ???????????????? ??????? ?????????? ???????:

1. **??? ???????** — ???????? ???????? ????, ??? ??? ???????????.
2. **??? ???????** — ???????? ??????????? ???????: `Application`, `Security`, `System`, ? ????? ??????? ????????? ?????????? (????????, `Windows PowerShell`).
3. **????????????? ???????** — ???? ??? ????????? Event ID, ??? ????????? ??????? ??????? ???????????.

?????: ?????????? ?? ????????? ??????????? ??????? ????????? ???????. ???? ???????? ??????? ??????? ? ???????, ??????? ?? ????? ????????.

4. ??????????? ??????? Windows: ??? ?????????? ? ?????? ???????

???????? ?? ???????? ??????????? ?????? ???????????? ??????, ????? ???????? ????????? ????????? ???????, ??????? ????? ?????????? ???????? ??? ??????????? ????.

4.1. ?????????????? ? ???? ? ???????

Event ID	Описание	Почему важно
4624	???????? ???? ? ???????	????????? ??????????? ????????? ????? (?????, ????????, ??????? ??????)
4625	????????? ??????? ?????	???????? ????????? ????????? ? ??????? ???????
4648	???? ? ?????? ???????? ???????	????? ????????? ?? ???????????? ?????????? ??? ????????????????? ??????? ??????
4672	???? ? ??????? ?????????????	????????? ?????????? — ??????????? ???????
4740	?????????? ??????? ??????	????? ???????????????? ? ???????????????? ????? ??? ???? ? ?????????????

4.2. ?????????? ???????? ???????? ? ????????

Event ID	Описание	Почему важно

4720	???????? ??????? ?????? ????????????	????????????????? ???????? ??????? ??????? — ??????? ????????? ???????
4728 / 4732	????????? ???????????? ? ?????? ? ??????? ?????????????????	????????? ????????? — ???? ?? ???????? ?????? ?????
4735	????????? ????????? ??????	????? ????????? ?? ?????????? ??????? ????????????
4756	????????? ???????????? ? ?????? ? ??????? ?????????????????	????????? 4728/4732

4.3. ????????? ??????? ? ????????? ???????

Event ID	Описание	Почему важно
1102	??????? ??????? ??????	??????? ?????? ????? ?????
4719	????????? ???????? ??????	????? ????????????? ??? ????????? ?????? ?????????? ???????
4616	????????? ????????? ???????	???????????? ??? «???????» ????????? ????? ???????

4.4. ?????? ? ???????? ? ??????????????????? ????????

Event ID	Описание	Почему важно
4660	???????? ???????	???????? ??????????? ?????? ??? ?????? ???????

Event ID	Описание	Почему важно
4674	??????? ???????? ? ????????????????? ????????	????? ????????? ?? ??????? ????????? ????????????????????? ???????

4.5. ???????? ? ???????

Event ID	Описание	Почему важно
4104	??????? ??????? ?????? ???????? PowerShell	????????? ???????????? ?????????? ???????????? ????????

4.6. ?????????????? ??????? ??? ???????????? ?????????? ??????? (Persistence)

Event ID	Описание
4698	???????? ?????????????? ??????
4699	???????? ?????????????? ??????
4700	????????? ?????????????? ??????
4701	?????????? ?????????????? ??????
4702	?????????? ?????????????? ??????

??? ??????? ????? ???????????? ???????????? ?????????????? ? ??????? ????? ?????????????? ?????????????.

---

5. ???????????? ?? ????????? ??????? ?????? Windows

??? ?????????? ?????? ??????? ???????? **??????????, ????? ???????? ?????? ??????????? ???? ????????? ? ??????? ????????????? ?????? ???????**.

????????????? ??????????? ????? ????????? ??????:

Категория аудита	Подкатегория	Рекомендация
Audit Account Logon	Audit Kerberos Authentication Service	????? ? ???????
Audit Account Management	Audit User Account Management, Audit Security Group Management	????? ? ???????
Audit Logon	Audit Logon	????? ? ???????
Audit Object Access	Audit File System, Audit Registry	????? ? ??????? (??? ?????????? ????????)
Audit Policy Change	Audit Policy Change	?????
Audit Privilege Use	Audit Sensitive Privilege Use	????? ? ???????
Audit System	Audit Security State Change, Audit System Integrity	?????

???????? ?????????? ?? ???????? ?????? ???????? ? ??????????? Microsoft.

---

7. ?????????? ? SIEM ? ???????????????? ????????

KICS for Nodes 4.5 ???????????? **???????? ??????? ? SIEM-???????**. ??? ?????????:

- ?????????????? ??????? ??????? ?? ???? ??????????? ?????.
- ???????????? ??????? ?? ?????? ??????????.
- ??????????? ?????????? SIEM ??? ??????????? ???????.

??? ???????? ???????? ? SIEM:

1. ? ???????? KICS for Nodes ???????? ? ?????? **??????? ? ?????????? ? ?????????? ? SIEM**.
2. ??????? ????? SIEM-???????, ???? ? ????????.

3. ??? ????????????? ????????? ?????????? ???????, ????? ? SIEM ???????????? ?????? ?????????? ?????? ???????.

??????????

??????????? ????????? ??????? ???????? ? Kaspersky Industrial CyberSecurity for Nodes 4.5 — ??? ?? ??????? ????????, ? ???????????? ???????, ????????? ????????? ??? ???????????? ?????? ????????, ??? ? ??????? ????? ??? ???????????? ??????.

???????????? ??????? ??????? ??????? ???????? ? ??????? ????? ????????????? ? ????????????? ???????????????? ????????. ????????? ??????? ???????? ?????? ???? ?????????? ??????: ??????? ??????? ??????? ????? ???????? ???, ??????? ?????? — ?????????? ?????. ??????? ? ???????????????? ??????, ?????????? ????????? ?? ? ?????????? ???????????????? — ? ?? ???????? ??????????? ?????????? ??????? ??????????? ????? ? ????? ???????????? ????.

Revision #3
Created 1 July 2026 04:02:15 by Alexey Panyukhin
Updated 1 July 2026 04:08:53 by Alexey Panyukhin