CIRCUIT & CAPITAL · FREE PACK · OCTOBER 2026

Grok Bot prompt pack for small IT, security and finance teams

6 ready-to-paste routine setups that read your data or public feeds on a schedule and send you a short report. Report-only: they never change, pay, reply to or delete anything.

INSIDE

1. Contract renewal watch (60 days ahead)
2. Weekly CISA KEV digest, filtered to your tools
3. Monthly SaaS spend and waste report
4. Vendor security news watch
5. Certificate and domain expiry watch
6. Inbox triage: invoices, renewals and price changes

HOW TO USE A SETUP

1. Replace every blank in [SQUARE BRACKETS] with your own details.
2. Paste the whole block into a Grok Bot chat. It creates the routine.
3. Ask it to run once now. Compare the result with the sample output.
4. Correct anything it got wrong in the same chat, then let the schedule run.

GROUND RULES

- One routine, one job. Do not merge setups into one long prompt.
- Never paste passwords or API keys into chat. Use a connected account or a shared file.
- Check the first few reports against the source. Agents can miss items or misread data.
- The KEV digest and expiry watch samples are real results from dry runs on Oct 31, 2026. The other samples use example data.

circuits.fit/grok-bot-pack · Questions: circuits50capital@circuits.fit · Want it run for you? circuits.fit/services/ai-staff, from $79 a month. This pack is general information, not legal or security advice.

Setup 1 of 6

Contract renewal watch (60 days ahead)

PURPOSE

Warns you while there is still time to cancel, cut seats or renegotiate. Most software contracts renew automatically and need written notice 30 to 90 days before the renewal date.

SUGGESTED SCHEDULE

Every Monday at 8:00 AM. Weekly is enough because the window is 60 days.

INPUTS YOU FILL IN

- [TIMEZONE], for example America/New_York
- [RENEWAL LIST]: a Google Sheet or CSV the bot can open, with columns Vendor, Annual cost, Renewal date, Notice period (days), Owner
- [DELIVERY]: where to send it, for example this chat or your email address

PASTE THIS INTO GROK BOT

```
Create a routine called "Renewal watch". Run it every Monday at 8:00 AM [TIMEZONE].
Each run:
1. Open [RENEWAL LIST]. Columns: Vendor, Annual cost, Renewal date, Notice period (days),
Owner.
2. For each row, notice deadline = Renewal date minus Notice period (days).
3. List every row whose notice deadline is today or within the next 60 days. Mark rows within
14 days as URGENT.
4. Separately list rows whose notice deadline has passed but whose renewal date has not,
marked PASSED (the notice window is probably missed; check the contract).
5. Sort by notice deadline, earliest first. For each row show: vendor, annual cost, renewal
date, notice deadline, days left, owner.
6. Put rows missing a renewal date or notice period under "Missing data". Do not guess them.
7. End with the total annual cost of the listed rows.
8. If nothing qualifies, send one line: "No notice deadlines in the next 60 days."
Send the result to [DELIVERY].
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
Renewal watch, Monday Nov 2, 2026 (example data)
URGENT
- Example CRM: $48,000/yr, renews Dec 31, 2026, notice deadline Nov 1 (60 days), PASSED 1 day
ago. Owner: Dana. Check whether notice can still be given.
- Help desk tool: $9,600/yr, renews Dec 15, notice deadline Nov 15 (30 days), 13 days left.
Owner: Sam.
Within 60 days
- Password manager: $3,000/yr, renews Feb 1, 2027, notice deadline Dec 3 (60 days), 31 days
left. Owner: Sam.
Missing data
- Design suite: no notice period in the sheet.
Total annual cost listed: $60,600
```

Setup 2 of 6

Weekly CISA KEV digest, filtered to your tools

PURPOSE

Tells you which newly listed actively exploited vulnerabilities touch the tools you actually run, and lists the rest in one line each so you can spot tools missing from your list.

SUGGESTED SCHEDULE

Every Monday at 7:30 AM. CISA adds entries most weekdays; a weekly digest catches the last 7 days.

INPUTS YOU FILL IN

- [TIMEZONE]
- [TOOL LIST]: one line per tool as Vendor: Product, for example Cisco: Secure Firewall ASA
- [ALIASES]: other vendor names to treat as the same, for example VMware = Broadcom, Atlassian = Jira
- [DELIVERY]

PASTE THIS INTO GROK BOT

```
Create a routine called "KEV digest". Run it every Monday at 7:30 AM [TIMEZONE].
Each run:
1. Download the CISA Known Exploited Vulnerabilities catalog JSON from
https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json. If the
download fails, report that and stop. Never invent CVEs.
2. Keep entries whose dateAdded is within the last 7 days, counting today.
3. My tools (Vendor: Product):
[TOOL LIST]
Vendor aliases: [ALIASES]
4. An entry is a MATCH when its vendorProject contains my vendor name or an alias, ignoring
case. Label it "Product match" when its product and my product share the main product word or
one contains the other (ESX and ESXi count as a match). Otherwise label it "Same vendor, check
product". When unsure, use the second label; do not drop the entry.
5. For each MATCH show: CVE ID, vendor, product, vulnerabilityName, dateAdded, dueDate,
knownRansomwareCampaignUse, and requiredAction in one line. Note that dueDate is the deadline
for US federal agencies and a useful guide for us.
6. Then list every other new entry as one line: CVE ID, vendor, product.
7. At the top, show the catalogVersion, the run date and the number of new entries. The
catalog can lag a day behind; that is normal.
Send the result to [DELIVERY].
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
KEV digest, Saturday Oct 31, 2026. Catalog version 2026.10.30, 10 new entries in the last 7
days.
Matches
- CVE-2026-118527 | Ivanti Connect Secure | Ivanti Connect Secure Generation of Predictable
Numbers or Identifiers Vulnerability | added 2026-10-30, due 2026-11-13 | ransomware use:
Unknown | Product match
  Action: Apply mitigations in accordance with vendor instructions.
- CVE-2026-111357 | Ivanti Connect Secure | Ivanti Connect Secure Missing Authentication for
Critical Function Vulnerability | added 2026-10-30, due 2026-11-02 | ransomware use: Unknown |
Product match
```

```
  Action: Apply mitigations in accordance with vendor instructions.
- CVE-2026-76418 | Cisco Secure Firewall ASA Software and Cisco Secure FTD Software | Cisco
Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL
Pointer Dereference Vulnerability | added 2026-10-29, due 2026-11-01 | ransomware use: Unknown
| Product match
  Action: Apply mitigations in accordance with vendor instructions.
- CVE-2026-41709 | Broadcom VMware ESX | Broadcom VMWare ESX Insufficient Logging
Vulnerability | added 2026-10-28, due 2026-11-11 | ransomware use: Unknown | Product match
  Action: Apply mitigations in accordance with vendor instructions.
Other new entries
- CVE-2026-97229 | GitLab Community Edition and Enterprise Edition
- CVE-2026-46300 | Linux Kernel
- CVE-2026-48356 | Adobe Commerce and Magento
- CVE-2026-111497 | Google Brotli
- CVE-2026-109618 | PHP Group PHP
- CVE-2026-109619 | PHP Group PHP
(Real output from a dry run against the live CISA feed, tool list: Microsoft: 365, Cisco:
Secure Firewall ASA, Ivanti: Connect Secure, VMware: ESXi, Fortinet: FortiGate, WordPress:
WordPress; alias VMware = Broadcom.)
```

Setup 3 of 6

Monthly SaaS spend and waste report

PURPOSE

One page each month on what software cost, what changed and where money is likely wasted, built from your card or expense export.

SUGGESTED SCHEDULE

The 2nd of each month at 9:00 AM, after card statements for the prior month close.

INPUTS YOU FILL IN

- [TIMEZONE]
- [SPEND EXPORT]: last month's card or expense export (CSV or sheet) with Date, Merchant, Amount
- [RENEWAL LIST]: the same list as the renewal watch, optional
- [SEAT DATA]: optional, paid seats and active users per tool
- [DELIVERY]

PASTE THIS INTO GROK BOT

```
Create a routine called "SaaS spend report". Run it on the 2nd of every month at 9:00 AM
[TIMEZONE].
Each run:
1. Open [SPEND EXPORT] for last month. Keep rows that are software or subscriptions (SaaS,
cloud, app stores, AI tools). List the rows you were unsure about separately.
2. Group by vendor. Show each vendor's total for last month and the month before, if the
earlier month is in the file.
3. Flag: (a) any vendor whose cost rose more than 10% month over month; (b) new vendors not
seen before; (c) two or more tools in the same category, such as two video call tools; (d)
vendors in the spend that are not on [RENEWAL LIST], if given; (e) tools where active users
are under 70% of paid seats, if [SEAT DATA] is given.
4. Give the total software spend for the month and the top 5 vendors by cost.
5. For each flag, give one suggested question for the tool's owner. Do not recommend
cancelling anything outright.
Send the result to [DELIVERY].
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
SaaS spend report, October 2026 (example data)
Total software spend: $7,412 across 31 vendors (September: $6,980)
Top 5: Cloud hosting $2,140, CRM $1,600, Office suite $1,104, Help desk $800, Design suite
$412
Flags
- Cloud hosting up 18% ($1,812 to $2,140). Ask: which project added usage?
- New vendor: an AI transcription tool, $60. Ask: who signed up, and is it approved?
- Two video call tools (Zoom $150, Webex $90). Ask: can one go at renewal?
- Not on renewal list: Design suite. Ask: what is the renewal date and notice period?
Unsure rows: "SQ *Bluebird" $45, possibly not software.
```

Setup 4 of 6

Vendor security news watch

PURPOSE

A short daily note when a vendor you depend on has a breach, outage or security advisory, with sources, so you hear it before the customer email does.

SUGGESTED SCHEDULE

Weekdays at 8:00 AM. Skip the message on days with nothing new.

INPUTS YOU FILL IN

- [TIMEZONE]
- [VENDORS]: your 10 to 20 most important vendors
- [ADVISORY PAGES]: each vendor's security advisory or status page URL, where you know it
- [DELIVERY]

PASTE THIS INTO GROK BOT

```
Create a routine called "Vendor security watch". Run it on weekdays at 8:00 AM [TIMEZONE].
Each run:
1. For each vendor in [VENDORS], check its page in [ADVISORY PAGES] if listed, then search the
web for news from the last 24 hours (72 hours on Mondays) with the vendor name plus breach,
vulnerability, advisory, outage or incident.
2. Keep only items with a source link from the vendor itself, a government agency (CISA, NCSC
and the like) or an established news outlet. Skip forums, rumor and vendor marketing.
3. For each item show: vendor, what happened in one sentence, whether customer action is
needed per the source, date, and the link.
4. Do not repeat items you already reported in an earlier run unless there is a material
update; mark those UPDATE.
5. If nothing qualifies, send nothing.
Send the result to [DELIVERY].
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
Vendor security watch, Friday Oct 30, 2026 (example)
- Ivanti: CISA added two Ivanti Connect Secure vulnerabilities to the KEV catalog on Oct 30,
one with a Nov 2 federal due date. Action needed: apply Ivanti's mitigations. Source: cisa.gov
KEV catalog.
- Cisco: CISA listed a Secure Firewall ASA / FTD vulnerability on Oct 29. Action needed if you
run ASA or FTD. Source: cisa.gov KEV catalog.
```

Setup 5 of 6

Certificate and domain expiry watch

PURPOSE

Catches a TLS certificate or domain registration before it lapses and takes your site or email down.

SUGGESTED SCHEDULE

Every Monday at 9:00 AM.

INPUTS YOU FILL IN

- [TIMEZONE]
- [DOMAINS]: every domain and subdomain you serve over HTTPS, one per line
- [DELIVERY]

PASTE THIS INTO GROK BOT

```
Create a routine called "Expiry watch". Run it every Monday at 9:00 AM [TIMEZONE].
Each run, for each name in [DOMAINS]:
1. Certificate: connect to https://NAME on port 443 and read the certificate the server
presents now (for example with openssl s_client). Record the expiry date (notAfter) and the
issuer. Do not use certificate-log sites such as crt.sh for this, because a newly issued
certificate may not be installed yet.
2. Registration: for the registered domain (example.com, not www.example.com), open
https://rdap.org/domain/DOMAIN and follow its redirect to the registry. Read the event whose
eventAction is "expiration". If that lookup fails, find the registry's RDAP address for the
ending (.com, .gov, .fit) in https://data.iana.org/rdap/dns.json and try DOMAIN there once. If
it still fails, or no expiration date is published, write "registration: not found" and keep
the certificate result.
3. Flag a certificate expiring within 30 days. If the issuer is Let's Encrypt or another
issuer of 90-day certificates, flag only within 14 days, because these normally auto-renew
around 30 days out; a flag means auto-renewal may be failing.
4. Flag a domain registration expiring within 60 days.
5. Show a table: name, certificate expiry, days left, issuer, domain expiry, days left, flag.
6. If the certificate check fails to connect, write ERROR and the error message in that
column. Do not drop the row.
7. Note at the top which names are flagged, or "No flags."
Send the result to [DELIVERY].
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
Expiry watch, Saturday Oct 31, 2026. No flags.
- circuits.fit | cert Jan 28, 2027 (89 days) | Let's Encrypt | domain Aug 31, 2027 (304 days)
| OK
- www.circuits.fit | cert Jan 28, 2027 (89 days) | Let's Encrypt | domain Aug 31, 2027 (304
days) | OK
- cisa.gov | cert Mar 03, 2027 (123 days) | DigiCert Inc | domain Nov 04, 2027 (369 days) | OK
- example.com | cert Dec 25, 2026 (55 days) | SSL Corporation | domain Aug 13, 2027 (286 days)
| OK
(Real output from a dry run against public sites.)
```

Setup 6 of 6

Inbox triage: invoices, renewals and price changes

PURPOSE

A daily list of money emails that need a decision: invoices, renewal notices, auto-renew reminders, price increases and failed payments, so none sit unread past a deadline.

SUGGESTED SCHEDULE

Weekdays at 4:00 PM.

INPUTS YOU FILL IN

- [TIMEZONE]
- [MAILBOX]: the connected inbox or label to read, for example a shared billing@ inbox
- [DELIVERY]

PASTE THIS INTO GROK BOT

```
Create a routine called "Money inbox triage". Run it on weekdays at 4:00 PM [TIMEZONE].
Each run:
1. Read emails in [MAILBOX] received since the last run (on Mondays, since Friday's run).
2. Pick out: invoices and bills, renewal or auto-renew notices, price or plan change notices,
failed or declined payment notices, and contract or terms-of-service changes. Ignore marketing
and newsletters.
3. For each, show: type, vendor, amount if stated, due date or renewal date if stated, one-
line summary, and a link to the email.
4. Sort by due date, earliest first. Mark anything due within 7 days as URGENT and any failed
payment as URGENT.
5. Flag a price increase or terms change on its own line, quoting the new price or the changed
clause.
6. If there is nothing, send one line: "No invoice or renewal mail today."
Send the result to [DELIVERY]. Do not reply to, forward, archive, label, pay or delete any
email.
This is report-only. Do not log into, change, reply to, pay, cancel or delete anything. If a
step fails or data is missing, say so in the report instead of guessing.
```

SAMPLE OUTPUT

```
Money inbox triage, Friday Oct 30, 2026 (example data)
URGENT
- Failed payment: Cloud hosting, $214, card declined, retry Nov 2. [link]
- Invoice: IT support contractor, $1,250, due Nov 4. [link]
Price change
- Office suite: business plan rises from $12.50 to $14 per user per month from Jan 1, 2027.
[link]
Other
- Renewal notice: Password manager, $3,000/yr, renews Feb 1, 2027. [link]
```

Next steps

Run the renewal watch for a month and you will have a list of notice deadlines. For a one-off review of that list with cut, renegotiate or keep recommendations, see the Renewal Audit ($199) at circuits.fit/services/renewal-audit.html.

If you would rather not run the routines yourself, the AI staff plan sets up and runs report-only agents for you: $79 a month for 1 agent or $149 a month for 3, cancel anytime. circuits.fit/services/ai-staff/

The weekly Circuit & Capital briefing covers renewals, security and AI spend for small teams. You are getting it because you asked for this pack; unsubscribe at any time from any issue.

© 2026 Circuit & Capital. You may use and adapt these setups inside your own organization.