

Vorteile einer offenen API

Workflow-Anbindung für verinice.veo

HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)

		HOW OFTEN YOU DO THE TASK					
		50/DAY	5/DAY	DAILY	WEEKLY	MONTHLY	YEARLY
HOW MUCH TIME YOU SHAVE OFF	1 SECOND	1 DAY	2 HOURS	30 MINUTES	4 MINUTES	1 MINUTE	5 SECONDS
	5 SECONDS	5 DAYS	12 HOURS	2 HOURS	21 MINUTES	5 MINUTES	25 SECONDS
	30 SECONDS	4 WEEKS	3 DAYS	12 HOURS	2 HOURS	30 MINUTES	2 MINUTES
	1 MINUTE	8 WEEKS	6 DAYS	1 DAY	4 HOURS	1 HOUR	5 MINUTES
	5 MINUTES	9 MONTHS	4 WEEKS	6 DAYS	21 HOURS	5 HOURS	25 MINUTES
	30 MINUTES		6 MONTHS	5 WEEKS	5 DAYS	1 DAY	2 HOURS
	1 HOUR		10 MONTHS	2 MONTHS	10 DAYS	2 DAYS	5 HOURS
	6 HOURS				2 MONTHS	2 WEEKS	1 DAY
	1 DAY					8 WEEKS	5 DAYS

Quelle: <https://xkcd.com/1205/>

Tools

+ Workflow-Engines:

+ Temporal, Airflow, Prefect, Pipedream, n8n, Microsoft Power Automate, Make, IFTTT, Zapier, **Windmill**

+ Integrierte Workflow-Features:

+ **KIX Pro**, Jira, ServiceNow, PagerDuty, Opsgenie, Zendesk, Asana, Monday.com, Slack, Smartsheet, Redmine, Zoho, MeisterTask, Podio, Basecamp, Bizagi, Wrike, Salesforce, Camunda, DocuSign, Workday, Drupal, Flowable, HubSpot CRM, SAP ERP, Oracle ERP Cloud, WordPress, Drupal, BambooHR, Workday, Marketo, Mailchimp, Camunda, Flowable, DocuSign, ...

Live-Demo:

1. IT-GS: Umsetzungsverantwortliche benachrichtigen
2. IT-GS: Zielobjekte aus externer Quelle beziehen
3. NIS2: Mehrstufiger Meldeprozess

Stars 11,922

Open-source developer platform and workflow engine

Turn scripts into auto-generated UIs, APIs and cron jobs.
Compose them as workflows or data pipelines.
Build complex, data-intensive apps with ease.

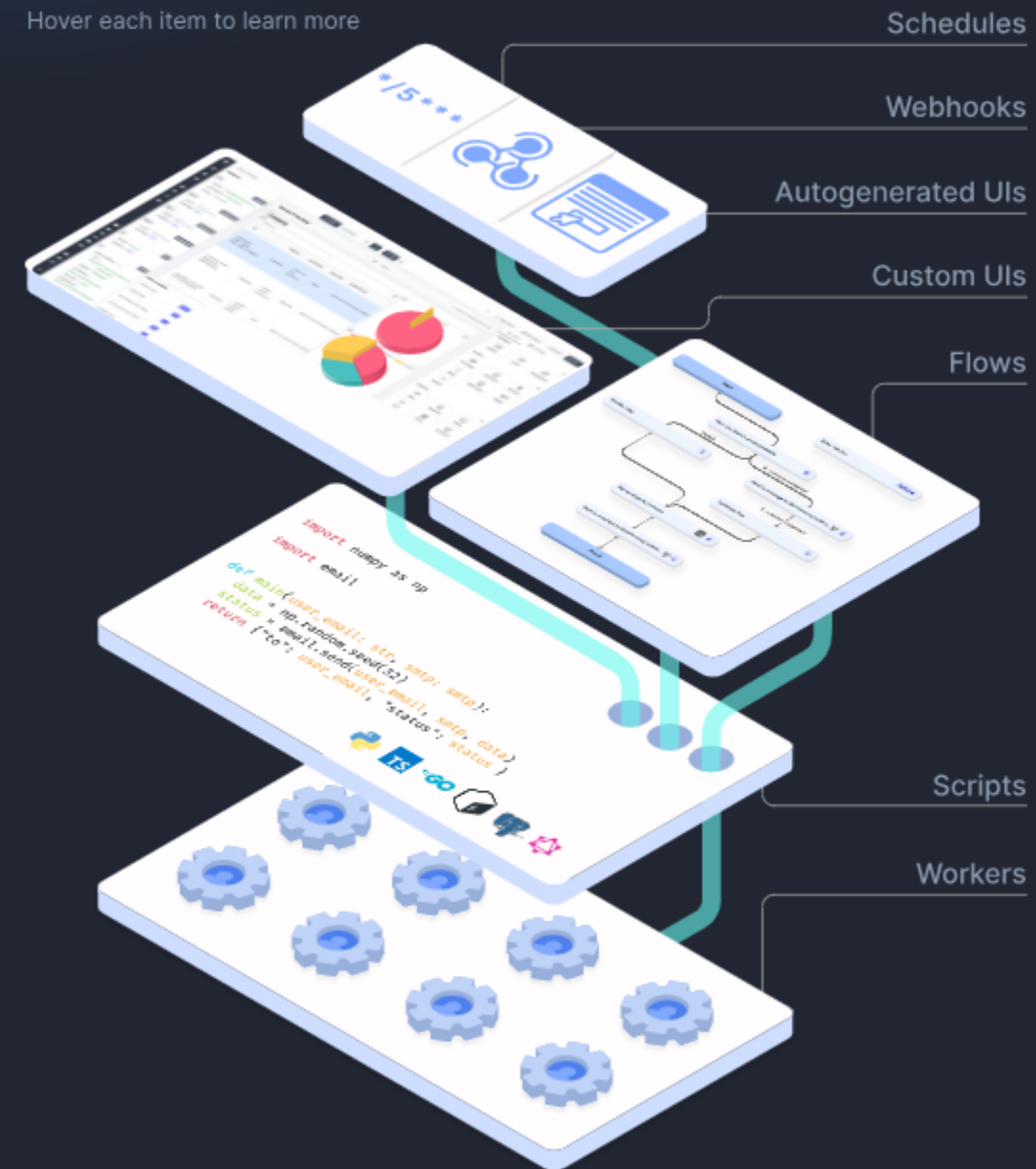
Write and deploy software 10x faster, and run it with the highest reliability and observability on the fastest self-hostable job orchestrator.

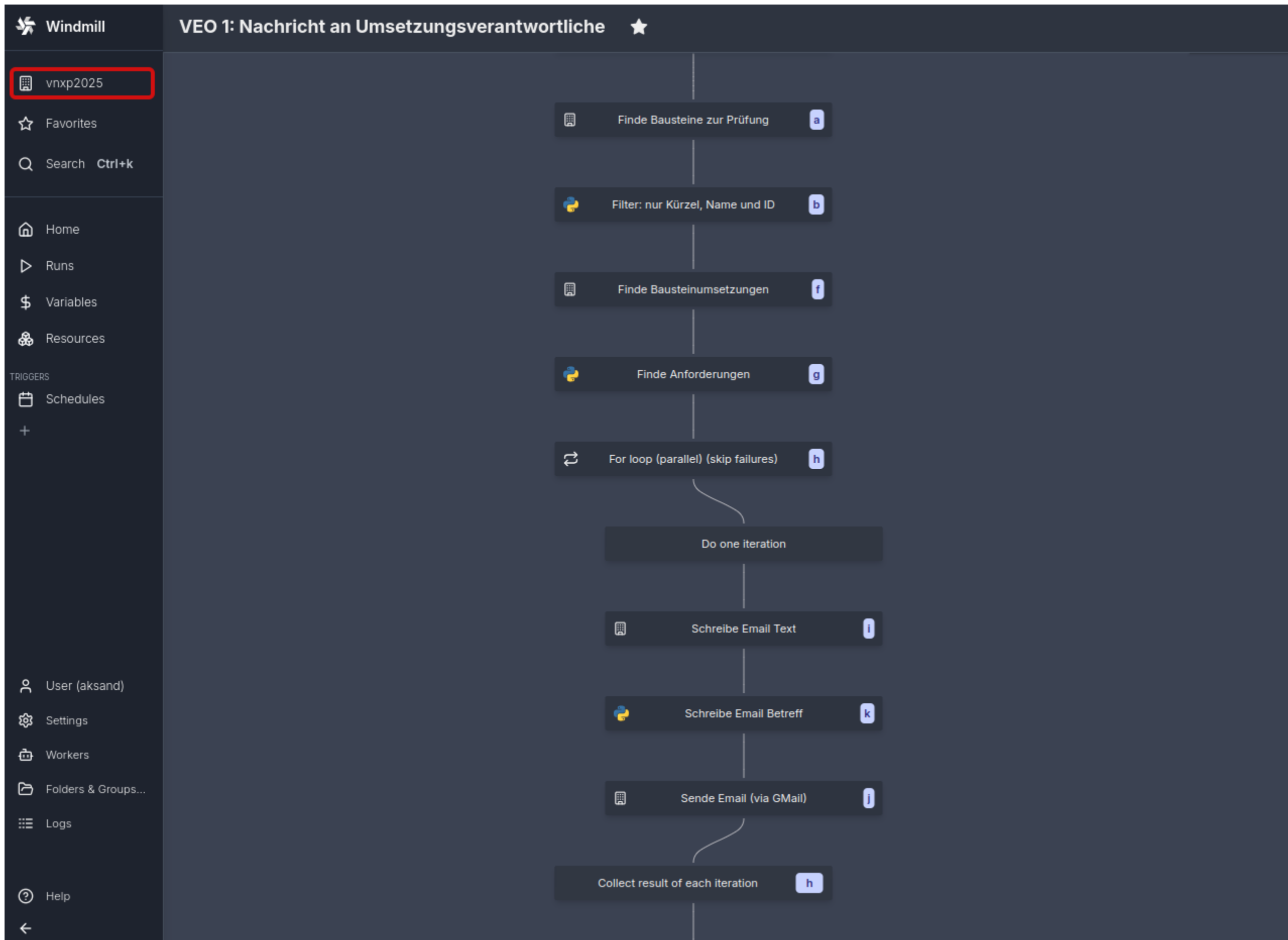
Try Windmill cloud

Self-host in 3 mins →

Backed by  Combinator

Hover each item to learn more





Unit
Standard-/Kernabsicherung ...

Domäne
IT-Grundschutz

- Informationen
- Anwendungen
- IT-Systeme
- ICS-Systeme
- IoT-Systeme
- Kommunikationsverbindungen
- Räume
- Personen
- Vorfälle
- Dokumente
- Maßnahmen
 - Alle
 - Bausteinfamilien
 - Bausteinschichten
 - Bausteine**
 - Anforderungen

Menü verstecken

Letzte Änderung: 05.02.2025, 22:49 von aksandbox
Erstellt: 03.02.2025, 20:27 von aksandbox
Keine Beschreibung vorhanden

TEILE IN SCOPE TEIL VON VERKNÜPFUNGEN **ZIELOBJekte**

Abkürzung	Name ↑		
📄	1 Büro	📄	🗑️
📄	2 Telearbeit im häuslichen Umfeld	📄	🗑️

Elemente pro Seite: 20 1-2 von 2 << < > >>

Abkürzung: 10 INF.7 Bearbeitungsreihenfolge: R2 Status*: Zur Prüfung

Name*: Büroarbeitsplatz

Beschreibung

Dokument

Hauptansprechpartner

+ VERKNÜPFUNG HINZUFÜGEN

IT-Grundschutz-Baustein
IT-Grundschutz-Kompendium

Beschreibung

Einleitung

Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein, eine oder mehrere Mitarbeitende aufhalten, um dort ihre Aufgaben zu erfüllen. In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum beschrieben.

Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die in Büroräumen bearbeitet werden.

ZURÜCKSETZEN

Abgrenzung und Modellierung

SPEICHERN

Unit
Standard-/Kernabsicherung ...

BAUSTEIN "BÜROARBEITSPLATZ" BEARBEITEN

Domäne
IT-Grundschutz

Abkürzung ↑	Vorgehensweise	Anforderung	Verantwortlich	Status	Umsetzungsherkunft
10 INF.7.A1	BASIS	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]		unbearbeitet	systemspezifisch
10 INF.7.A2	BASIS	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]		unbearbeitet	systemspezifisch
10 INF.7.A3	STANDARD	Fliegende Verkabelung	PER-329 HH Hans Haustechniker	unbearbeitet	systemspezifisch
10 INF.7.A5	STANDARD	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]		unbearbeitet	systemspezifisch
10 INF.7.A6	STANDARD	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	PER-330 MM Manfred Mitarbeiter	unbearbeitet	systemspezifisch
10 INF.7.A7	STANDARD	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]		unbearbeitet	systemspezifisch
10 INF.7.A8	ERHÖHT	Einsatz von Diebstahlsicherungen [Mitarbeitende]		unbearbeitet	systemspezifisch

Elemente pro Seite: 20 1-7 von 7 << < > >>

- Unit
Standard-/Kernabsicherung ...
- Domäne
IT-Grundschutz
- Informationen
- Anwendungen
- IT-Systeme
- ICS-Systeme
- IoT-Systeme
- Kommunikationsverbindungen
- Räume
- Personen
- Vorfälle

BAUSTEIN "BÜROARBEITSPLATZ" BEARBEITEN						
Abkürzung ↑	Vorgehensweise	Anforderung	Verantwortlich	Status	Umsetzungsherkunft	
10 INF.7.A1	BASIS	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]		unbearbeitet	systemspezifisch	
10 INF.7.A2	BASIS	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]		unbearbeitet	systemspezifisch	
10 INF.7.A3	STANDARD	Fliegende Verkabelung	PER-331 ZZ Zacharias Zuhause	unbearbeitet	systemspezifisch	
10 INF.7.A5	STANDARD	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]		unbearbeitet	systemspezifisch	
10 INF.7.A6	STANDARD	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	PER-331 ZZ Zacharias Zuhause	unbearbeitet	systemspezifisch	
10 INF.7.A7	STANDARD	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]		unbearbeitet	systemspezifisch	
10 INF.7.A8	ERHÖHT	Einsatz von Diebstahlsicherungen [Mitarbeitende]		unbearbeitet	systemspezifisch	

Von alexander@koderman.de
An workflowworker+zacharias@proton.me

Aufgabe für "PER-331 ZZ Zacharias Zuhause": 1

Bitte bearbeiten Sie CTL-21849 10 INF.7.A6 Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte].

Sie können die Umsetzung unter folgendem Link direkt dokumentieren:

<https://veo-web.sandbox.verinice.com/3d47b7d7-29f9-42fb-9414-0010b5e4ae23/domains/c4503929-0737-4875-8b46-dfba2512b3f/compliance?type=asset&targetObject=ab045637-355c-43a9-8c3f-0dbed1ac07fd&control=21866259-ea3f-472a-88e7-78980c2e1259>

Mit freundlichen Grüßen,
Ihr Sicherheitsbeauftragter

Von alexander@koderman.de
An workflowworker+manfred@proton.me

Aufgabe für "PER-330 MM Manfred Mitarbeiter": 2

Bitte bearbeiten Sie CTL-21849 10 INF.7.A6 Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte].

Sie können die Umsetzung unter folgendem Link direkt dokumentieren:

<https://veo-web.sandbox.verinice.com/3d47b7d7-29f9-42fb-9414-0010b5e4ae23/domains/c4503929-0737-4875-8b46-dfba2512b3f/compliance?type=asset&targetObject=ceb393e9-3a0f-4235-aec2-b9c618caf5ca&control=21866259-ea3f-472a-88e7-78980c2e1259>

Mit freundlichen Grüßen,
Ihr Sicherheitsbeauftragter

Von alexander@koderman.de
An workflowworker+hans@proton.me

Aufgabe für "PER-329 HH Hans Haustechniker": 1

Bitte bearbeiten Sie CTL-22580 10 INF.7.A3 Fliegende Verkabelung.

Sie können die Umsetzung unter folgendem Link direkt dokumentieren:

<https://veo-web.sandbox.verinice.com/3d47b7d7-29f9-42fb-9414-0010b5e4ae23/domains/c4503929-0737-4875-8b46-dfbea2512b3f/compliance?type=asset&targetObject=ceb393e9-3a0f-4235-aec2-b9c618caf5ca&control=21866259-ea3f-472a-88e7-78980c2e1259>

Mit freundlichen Grüßen,
Ihr Sicherheitsbeauftragter

Von alexander@koderman.de
An workflowworker+zacharias@proton.me

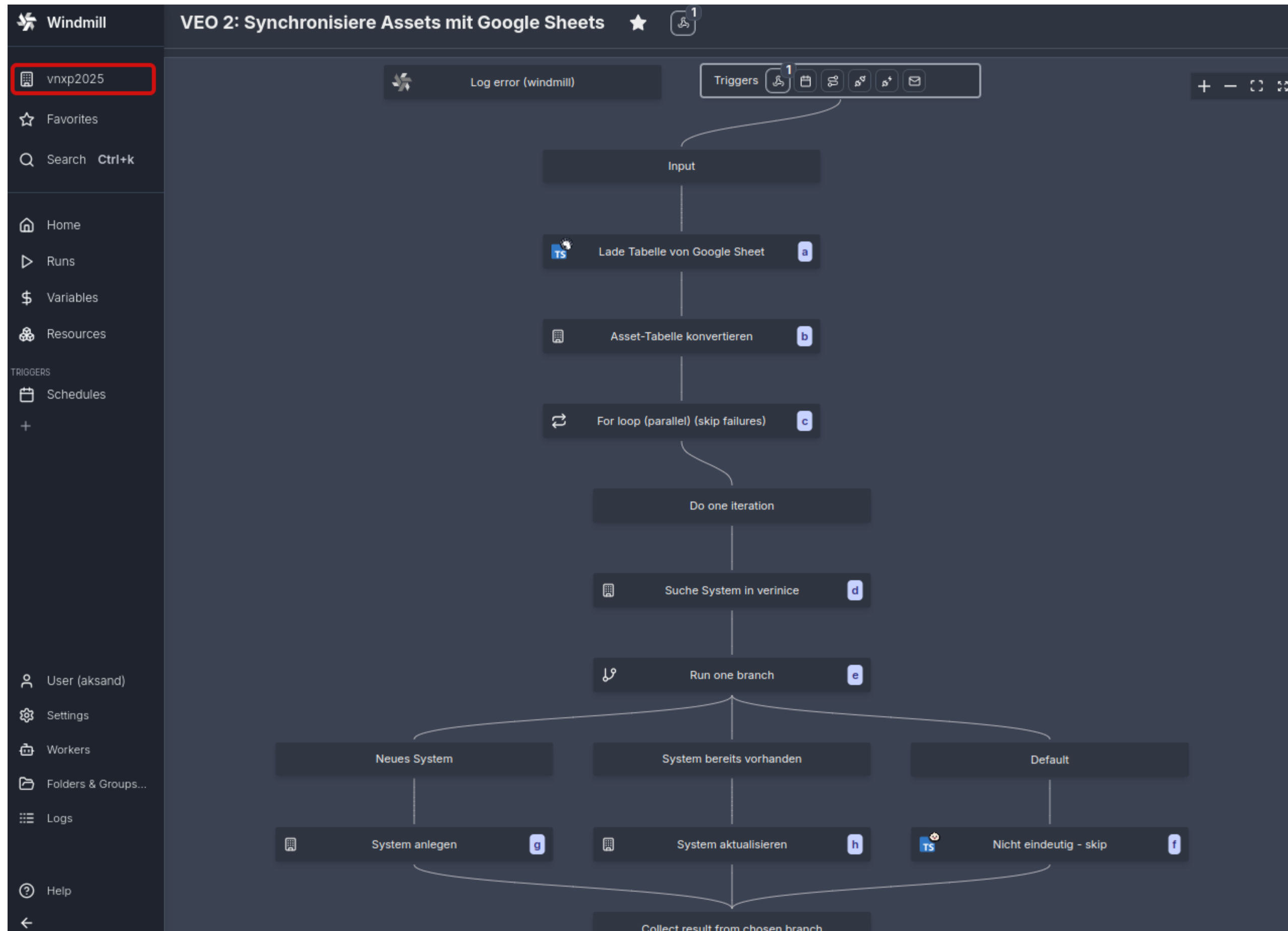
Aufgabe für "PER-331 ZZ Zacharias Zuhause": 2

Bitte bearbeiten Sie CTL-22580 10 INF.7.A3 Fliegende Verkabelung.

Sie können die Umsetzung unter folgendem Link direkt dokumentieren:

<https://veo-web.sandbox.verinice.com/3d47b7d7-29f9-42fb-9414-0010b5e4ae23/domains/c4503929-0737-4875-8b46-dfbea2512b3f/compliance?type=asset&targetObject=ab045637-355c-43a9-8c3f-0dbed1ac07fd&control=21866259-ea3f-472a-88e7-78980c2e1259>

Mit freundlichen Grüßen,
Ihr Sicherheitsbeauftragter



Serverliste

Menüs

100%

Inventar-ID	Hostname	IP-Adresse	Standort	Betriebssystem	Prozessor	RAM	Speicher	Seriennummer	Hersteller	Modell	Kaufdatum	Garantie bis	Status	Typ
S001	srv01.dc1.example.com	10.0.0.1	Rechenzentrum A	Ubuntu Server 20.04 LTS	Intel Xeon E5-2620 v4	0GB	2x1TB SSD	SN-A12345B67890	Dell	PowerEdge R740	2019-03-12	2024-03-12	Wartung	Physisch
S002	srv02.dc1.example.com	10.0.0.2	Rechenzentrum A	Windows Server 2019	Intel Xeon E5-2640 v4	128GB	4x1TB SATA	SN-B23456C78901	HP	ProLiant DL380 Gen10	2020-06-15	2025-06-15	In Betrieb	Physisch
S003	srv03.dc2.example.com	10.0.1.1	Rechenzentrum B	CentOS 7	AMD EPYC 7302P	32GB	2x500GB SSD	SN-C34567D89012	Lenovo	ThinkSystem SR650	2018-11-20	2023-11-20	In Betrieb	Physisch

Unit
Workflow Demo

Domäne
IT-Grundschutz

- Dashboard
- Editoren
- Objekte
 - Scopes
 - Prozesse
 - Assets
 - Alle

FILTER OBJEKTTYP ASSET SUBTYP IT-SYSTEM STATUS NEU

Suche
Name & Abkürzung = s0

Designator	Abkürzung	Name ↑	Status	Letzte Änderung	Bearbeiter	
AST-941	S001	srv01.dc1.example.com	Neu	11.02.2025, 10:20	aksandbox	
AST-940	S002	srv02.dc1.example.com	Neu	11.02.2025, 10:20	aksandbox	
AST-939	S003	srv03.dc2.example.com	Neu	11.02.2025, 10:20	aksandbox	

Elemente pro Seite: 20 1-3 von 3

Unit
Workflow Demo

Domäne
IT-Grundschutz

Dashboard

Editoren

Objekte

- Scopes
- Prozesse
- Assets
- Alle
- Informationen
- Anwendungen
- IT-Systeme**
- ICS-Systeme
- IoT-Systeme
- Kommunikationsverbindungen
- Räume

Letzte Änderung: 11.02.2025, 10:20 von aksandbox
Erstellt: 10.02.2025, 11:50 von aksandbox

Standort: Rechenzentrum A Betriebssystem: Ubuntu Server 20.04 LTS Prozessor: Intel Xeon E5-2620 v4 RAM: 0GB Speicher: 2x1TB SSD Seriennummer: SN-A12345B67890 Hersteller: Dell Modell: PowerEdge R740 Kaufdatum: 2019-03-12 Garantie bis: 2024-03-12 Typ: Physisch

< **TEILE** IN SCOPE TEIL VON VERKNÜPFUNGEN >

Abkürzung	Name ↑	Status

Elemente pro Seite: 20 0-0 von 0 << < > >>

Name*
srv01.dc1.example.com

Beschreibung
Standort: Rechenzentrum A
Betriebssystem: Ubuntu Server 20.04 LTS
Prozessor: Intel Xeon E5-2620 v4
RAM: 0GB
Speicher: 2x1TB SSD
Seriennummer: SN-A12345B67890
Hersteller: Dell
Modell: PowerEdge R740
Kaufdatum: 2019-03-12
Garantie bis: 2024-03-12
Typ: Physisch

Dokument

Netzplan

+ VERKNÜPFUNG HINZUFÜGEN

Details

Anzahl
Betriebsstadium
Reparatur

ZURÜCKSETZEN SPEICHERN



Serverliste

Menüs

100%

123

10

B I A

N2 In Betrieb

Inventar-ID	Hostname	IP-Adresse	Standort	Betriebssystem	Prozessor	RAM	Speicher	Seriennummer	Hersteller	Modell	Kaufdatum	Garantie bis	Status	Typ
S001	srv01_dc1.example.com	10.0.0.1	Rechenzentrum A	Ubuntu Server 20.04 LTS	Intel Xeon E5-2620 v4	64GB	2x1TB SSD	SN-A12345B67890	Dell	PowerEdge R740	2019-03-12	2024-03-12	In Betrieb	Physisch
S002	srv02_dc1.example.com	10.0.0.2	Rechenzentrum A	Windows Server 2019	Intel Xeon E5-2640 v4	128GB	4x1TB SATA	SN-B23456C78901	HP	ProLiant DL380 Gen10	2020-06-15	2025-06-15	In Betrieb	Physisch
S003	srv03_dc2.example.com	10.0.1.1	Rechenzentrum B	CentOS 7	AMD EPYC 7302P	32GB	2x500GB SSD	SN-C34567D89012	Lenovo	ThinkSystem SR650	2018-11-20	2023-11-20	In Betrieb	Physisch

Unit
Workflow Demo

Domäne
IT-Grundschatz

Dashboard

Editoren

Objekte

- Scopes
- Prozesse
- Assets
- Alle
- Informationen
- Anwendungen
- IT-Systeme**
- ICS-Systeme
- IoT-Systeme
- Kommunikationsverbindungen
- Räume

Letzte Änderung: 16.02.2025, 15:30 von aksandbox
Erstellt: 10.02.2025, 11:50 von aksandbox

Standort: Rechenzentrum A Betriebssystem: Ubuntu Server 20.04 LTS Prozessor: Intel Xeon E5-2620 v4 RAM: 64GB Speicher: 2x1TB SSD Seriennummer: SN-A12345B67890 Hersteller: Dell Modell: PowerEdge R740 Kaufdatum: 2019-03-12 Garantie bis: 2024-03-12 Typ: Physisch

< **TEILE** IN SCOPE TEIL VON VERKNÜPFUNGEN >

Abkürzung	Name ↑	Status

Elemente pro Seite: 20 0-0 von 0 << < > >>

Name*
srv01.dc1.example.com

Beschreibung
 Standort: Rechenzentrum A
 Betriebssystem: Ubuntu Server 20.04 LTS
 Prozessor: Intel Xeon E5-2620 v4
 RAM: 64GB
 Speicher: 2x1TB SSD
 Seriennummer: SN-A12345B67890
 Hersteller: Dell
 Modell: PowerEdge R740
 Kaufdatum: 2019-03-12
 Garantie bis: 2024-03-12
 Typ: Physisch

Dokument 🗑️

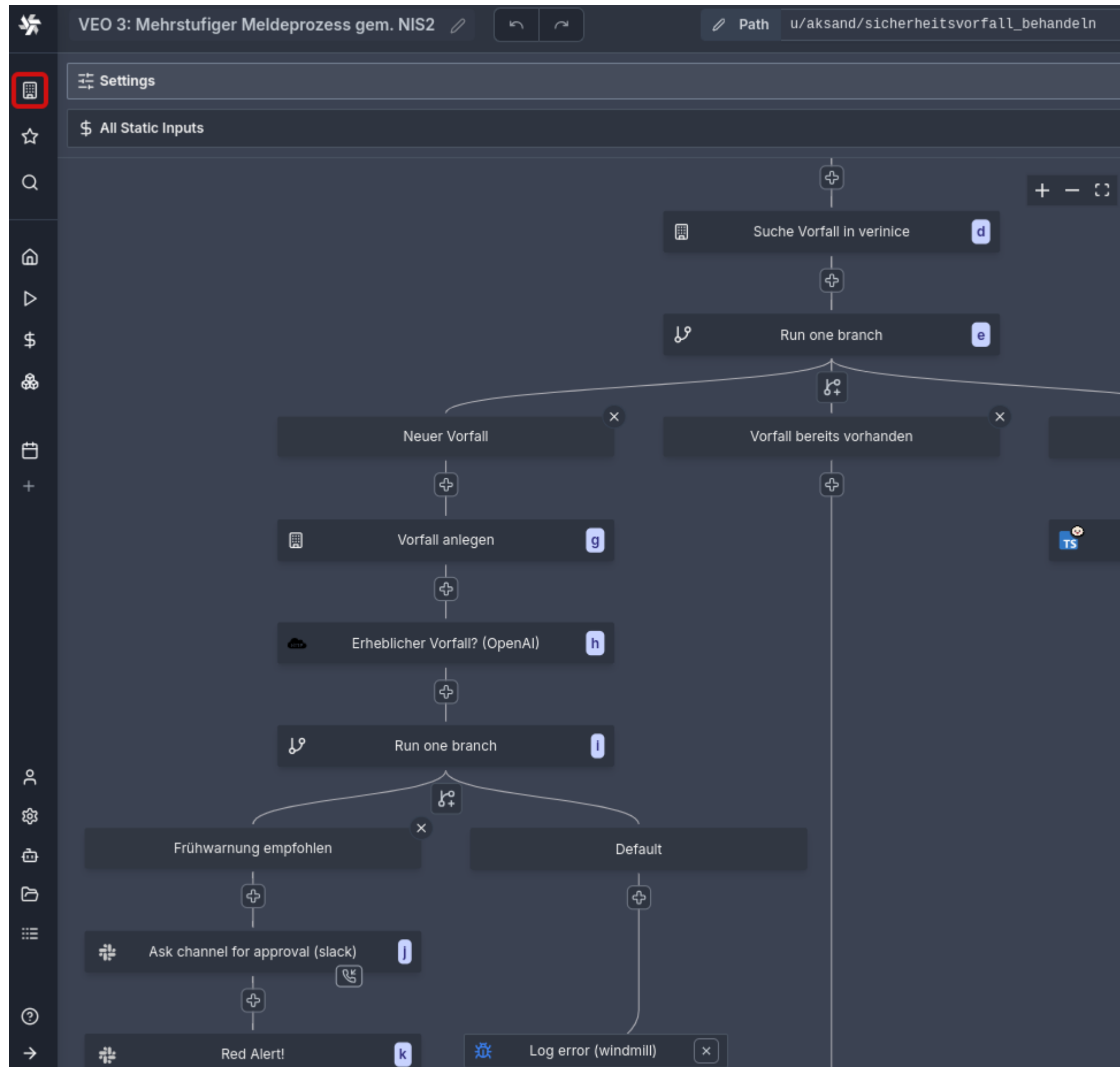
Netzplan ▼ 🗑️

+ VERKNÜPFUNG HINZUFÜGEN

Details

Anzahl Betriebsstadium

Betrieb SPEICHERN



The screenshot shows a Slack workspace named 'vnxp2025'. The left sidebar contains navigation options like Home, DMs, and Channels. The main area is the '# support' channel. A modal window titled 'Sicherheitsvorfall' (Security Incident) is open, containing a text input field for a description, a list of incident types with checkboxes, and a section for affected systems. The modal has 'Schließen' (Close) and 'Senden' (Send) buttons at the bottom. In the background, a message from 'akoderman' is visible, and a system message states 'Canvas wurde aktualisiert'.

Sicherheitsvorfall

Kurzbeschreibung des Vorfalls

Schreibe etwas

Bitte geben Sie eine prägnante Beschreibung des Vorfalls.

Art des Sicherheitsvorfalls

- Datenverlust
- Unbefugter Zugriff
- Malware/Virus
- Phishing-Angriff
- Verdacht fu Insider-Angriff
- Sicherheitslücke in einer Anwendung
- DDos Angriff
- Andere

Betroffene Systeme/Dienste

Schließen Senden

← → 🕒 vnxp2025 durchsuchen 🔍

vnxp2025 📄

🏠 Home Erhalte 50 % Rabatt auf Slack Pro
Dieses Angebot ist noch 4 Tage gültig

🗨️ DMs

🔔 Aktivität

📺 Automatisierungen

⋮ Mehr

📁 Huddles

📁 Channels

- # alle-in-neuer-workspace
- # red-alert
- # sozial
- # support

vnxp2025

+ Channels hinzufügen

📁 Direktnachrichten

- akoderman du

+ Leute hinzufügen

📁 Apps

- Anfrageformular
- Begrüßungsnachricht
- Google Sheets
- PagerDuty
- Sicherheitsvorfall melden
- Windmill
- Wöchentliche Kennenlernspiele
- + Apps hinzufügen

vnxp2025 👤 1 🗨️ Huddle ⋮

🗨️ Nachrichten 📁 Geteilte Ressourcen ⚡ Workflows 📁 Dateien +

📅 Samstag, 8. Februar ▾

👍 Reagieren 🗨️ Antworten ⋮

Sicherheitsvorfall melden WORKFLOW 21:46 Uhr

Art des Sicherheitsvorfalls
Phishing-Angriff

Auswirkungen des Vorfalls
Daten wurden offengelegt, Datenintegrität beeinträchtigt

Betroffene Systeme/Dienste
Mein PC


Ergriffene Sofortmaßnahmen
Panik.

Kurzbeschreibung des Vorfalls
Auf Phishing Link geklickt

Wurde der Vorfall bereits an andere Stellen gemeldet?
Nein

akoderman | 2025-02-08 21_46_01-phishing beispiel dhl - Google Search.png ▾

Betreff: DHL - Versandbenachrichtigung Sendungsnummer 057279013579



B *I* 🔗 📁 📁 📁 </> 🗑️

Nachricht an #vnxp2025

+ Aa 😊 @ 📁 🗣️ 📄

vnxp2025

22 Tage im Probe-Abo übrig

- Home
- DMs
- Aktivität
- Später
- Automatisierungen
- Mehr

Threads

Huddles

Entwürfe & Gesendet

Favoriten

support

vnxp2025

Channels

alle-in-neuer-workspace

red-alert

sozial

+ Channels hinzufügen

Direktnachrichten

akoderman du

+ Leute hinzufügen

Apps

Anfrageformular

Begrüßungsnachricht

Google Sheets

PagerDuty

Sicherheitsvorfall melden

Windmill

+ Apps hinzufügen

vnxp2025

Nachrichten Geteilte Ressourcen Workflows Dateien +

Gestern

Hi, I'm having trouble logging into my account.
Hello @customer_john, I'm here to help. What error do you see?
It says 'Invalid credentials' even though I'm sure my password is correct.
Have you tried resetting your password?
Yes, but I didn't receive the reset email.
Hi @customer_john, please check your spam folder or let me know if it's still not arriving.
I'm having issues with the mobile app. It crashes when I try to open the dashboard.
Hey @customer_sarah, can you confirm which device and OS version you're using?
I'm using [redacted]

Heute

Neu

https://veo-web.sandbox.verinice.com/3d47b7d7-29f9-42fb-9414-0010b5e4ae23/domains/0531d166-b8f7-40b5-a855-228233980b86/incidents/inc_securityincident/bcf62f0e-da93-4a56-bbc3-0c155eb489d6

INC-SRDQZ Auf Phishing Link geklickt

Windmill APP 15:32 Uhr

[verinice.cloud] Vorfall wurde angelegt. Bitte bewerten:
[INC-SROW6W RAT Tool auf meinem Rechner entdeckt](#)

15:33 Uhr [verinice.cloud] Vorfall wurde angelegt. Bitte bewerten:
[INC-SRDQZ Auf Phishing Link geklickt](#)

Unit
Workflow Demo

Domäne
NIS2

Dashboard

Editoren

Objekte

Scopes

Prozesse

Assets

Personen

Vorfälle

Alle

Sicherheitsvorfälle

Dokumente

Maßnahmen

Katalog

Reports

Letzte Änderung: 16.02.2025, 15:33 von aksandbox
Erstellt: 16.02.2025, 15:33 von aksandbox

Kurzbeschreibung des Vorfalls: Auf Phishing Link geklickt
Art des Sicherheitsvorfalls: Phishing-Angriff
Betroffene Systeme/Dienste: Mein PC
Ergriffene Sofortmaßnahmen: Panik...
Auswirkungen des Vorfalls: Daten wurden offengelegt, Datenintegrität beeinträchtigt
Wurde der Vorfall bereits an andere Stellen gemeldet?: Nein
Eingereicht von: akoderman

TEILE IN SCOPE TEIL VON VERKNÜPFUNGEN

Abkürzung	Name ↑	Status
-----------	--------	--------

Elemente pro Seite: 20 0-0 von 0

Allgemeine Angaben

Abkürzung: INC-SRDQ TZ Status*: Neu

Name*: Auf Phishing Link geklickt

Beschreibung
Kurzbeschreibung des Vorfalls: Auf Phishing Link geklickt
Art des Sicherheitsvorfalls: Phishing-Angriff
Betroffene Systeme/Dienste: Mein PC
Ergriffene Sofortmaßnahmen: Panik...
Auswirkungen des Vorfalls: Daten wurden offengelegt, Datenintegrität beeinträchtigt
Wurde der Vorfall bereits an andere Stellen gemeldet?: Nein
Eingereicht von: akoderman

Dokument
<https://vnxp2025.slack.com/files/U08CTCB86BT/F08CHB353L4/2025-01>

Art des Vorfalls
 Sicherheitsvorfall? Meldungsart: Meldung

ZURÜCKSETZEN SPEICHERN



Windmill APP 15:32 Uhr

[verinice.cloud] Vorfall wurde angelegt. Bitte bewerten:
[INC-SROW6W RAT Tool auf meinem Rechner entdeckt](#)

[verinice.cloud] Vorfall wurde angelegt. Bitte bewerten:
[INC-SRDQTZ Auf Phishing Link geklickt](#)

[verinice.cloud] Vorfall wurde angelegt. Bitte bewerten:
[INC-SRHLMS Trojanerangriff: zentrale Kundendatenbank entwendet, nahezu alle Kunden betroffen.](#)

[verinice.cloud] Erinnerung: Frühwarnung Art. 23, IV, a) NIS2 erforderlich bis spätestens 11.02.2025 21:42 +01:00

[verinice.cloud] Erinnerung: Meldung, Art. 23, IV, b) NIS2 erforderlich bis spätestens 13.02.2025 21:42 +01:00

B I

Nachricht an #vnxp2025

+ Aa @





Windmill APP 15:36 Uhr

[verinice.cloud] Achtung bei **Vorfall INC-SRHLMS Trojanerangriff: zentrale Kundendatenbank entwendet, nahezu alle Kunden betroffen.**

Möglicherweise **Frühwarnung** gem. Art. 23, IV, a) NIS2 erforderlich! **Begründung:**

Es handelt sich um einen erheblichen Sicherheitsvorfall, da der Trojanerangriff auf die zentrale Kundendatenbank zu einem Datenverlust geführt hat, der nahezu alle Kunden betrifft. Die Offenlegung von Daten kann erhebliche materielle und immaterielle Schäden für die betroffenen Personen nach sich ziehen, was den Vorfall schwerwiegend macht. Zudem könnte der Vorfall zu Reputationsschäden für das Unternehmen führen, was ebenfalls finanzielle Verluste zur Folge haben kann. Die Tatsache, dass noch keine Sofortmaßnahmen ergriffen wurden, erhöht das Risiko weiterer Schäden. Daher erfüllt dieser Vorfall die Kriterien eines erheblichen Sicherheitsvorfalls gemäß Art. 23, IV, a) NIS2.

B *I*

Nachricht an #red-alert

Aa

Unit
Workflow Demo

Domäne
NIS2

Dashboard

Editoren

Objekte

Scopes

Prozesse

Assets

Personen

Vorfälle

Alle

Sicherheitsvorfälle

Dokumente

Maßnahmen

Katalog

Reports

Letzte Änderung: 16.02.2025, 15:36 von aksandbox
Erstellt: 16.02.2025, 15:36 von aksandbox

Kurzbeschreibung des Vorfalls: Trojanerangriff: zentrale Kundendatenbank entwendet, nahezu alle Kunden betroffen. Art des Sicherheitsvorfalls: Datenverlust, Malware/Virus
Betroffene Systeme/Dienste: Kunden-Datenbank
Ergriffene Sofortmaßnahmen: noch keine
Auswirkungen des Vorfalls: Daten wurden offengelegt, Reputationsschäden
Wurde der Vorfall bereits an andere Stellen gemeldet?: nein
Eingereicht von: akoderman

TEILE IN SCOPE TEIL VON VERKNÜPFUNGEN

Abkürzung	Name ↑	Status

Elemente pro Seite: 20 0-0 von 0

Betroffene Geschäftsprozesse

+ VERKNÜPFUNG HINZUFÜGEN

Mögliche Folgen und Auswirkungen

Mögliche Folgen und Auswirkungen

Es handelt sich um einen erheblichen Sicherheitsvorfall, da der Trojanerangriff auf die zentrale Kundendatenbank zu einem Datenverlust geführt hat, der nahezu alle Kunden betrifft. Die Offenlegung von Daten kann erhebliche materielle und immaterielle Schäden für die betroffenen Personen nach sich ziehen, was den Vorfall schwerwiegend macht. Zudem könnte der Vorfall zu Reputationsschäden für das Unternehmen führen, was ebenfalls finanzielle Verluste zur Folge haben kann. Die Tatsache, dass noch keine Sofortmaßnahmen ergriffen wurden, erhöht das Risiko weiterer Schäden. Daher erfüllt dieser Vorfall die Kriterien eines erheblichen Sicherheitsvorfalls gemäß Art. 23, IV, a NIS2.

Erheblicher Sicherheitsvorfall? Einschätzung des Schweregrades: Erheblich

Meldung an Empfänger und Öffentlichkeit

Wurden die betroffenen Empfänger über den Sicherheitsvorfall informiert?

Ist eine öffentliche Bekanntmachung über den Sicherheitsvorfall erfolgt?

ZURÜCKSETZEN Gegenmaßnahmen SPEICHERN

Kontakt

SerNet GmbH

Bahnhofsallee 1b
37081 Göttingen

Tel: +49 (551) 370000-0

E-Mail: marketing@sernet.de

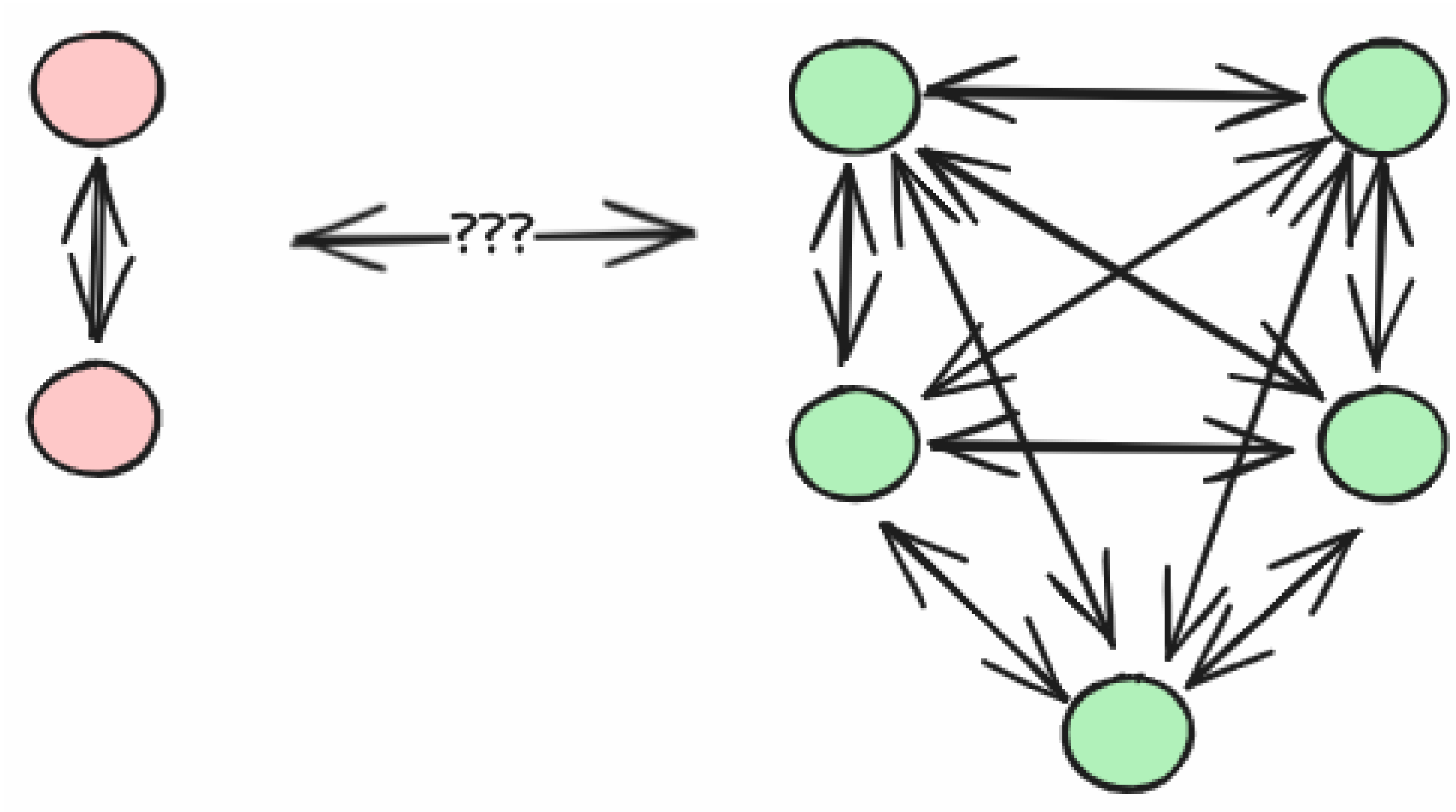
SerNet

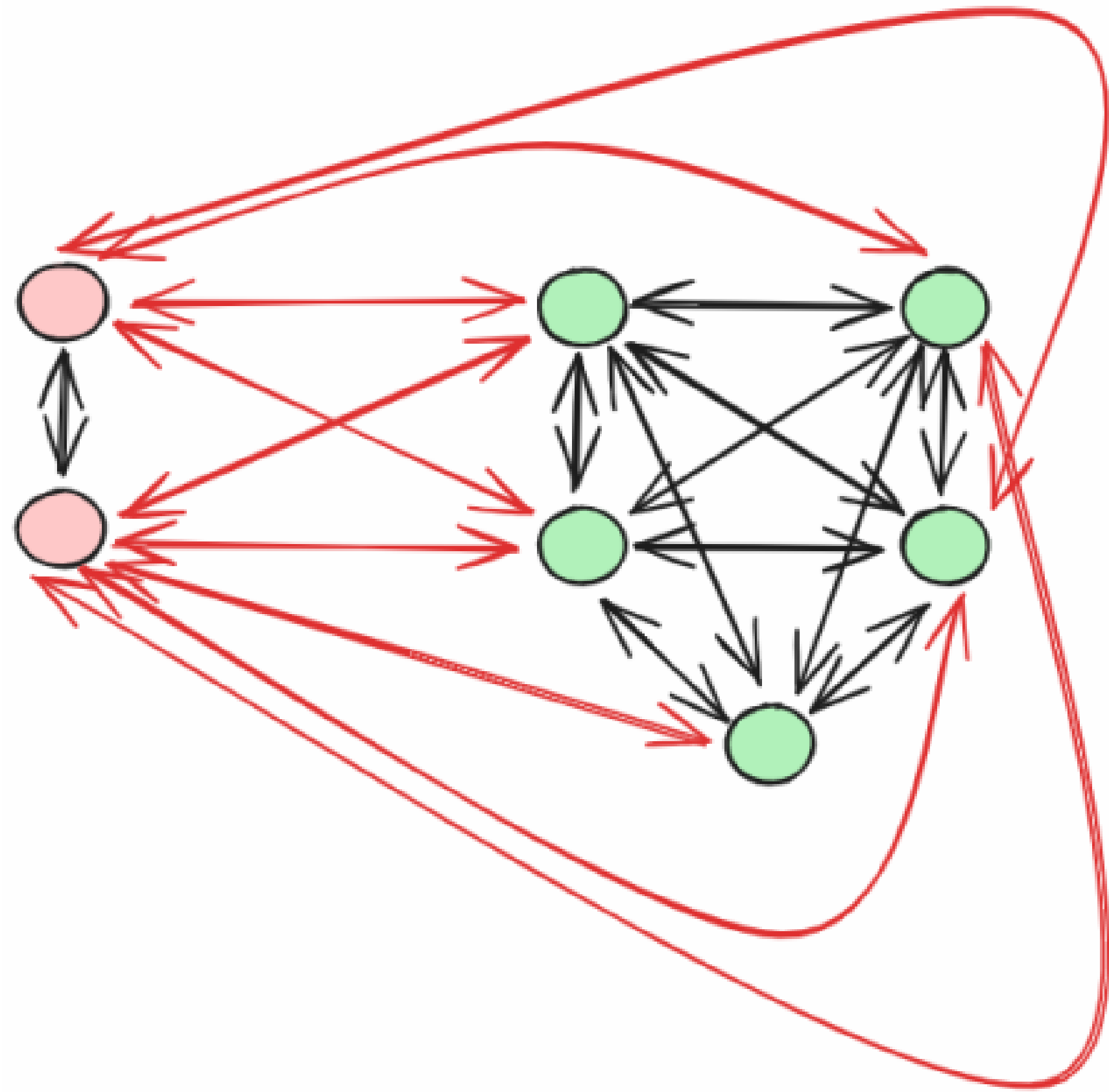


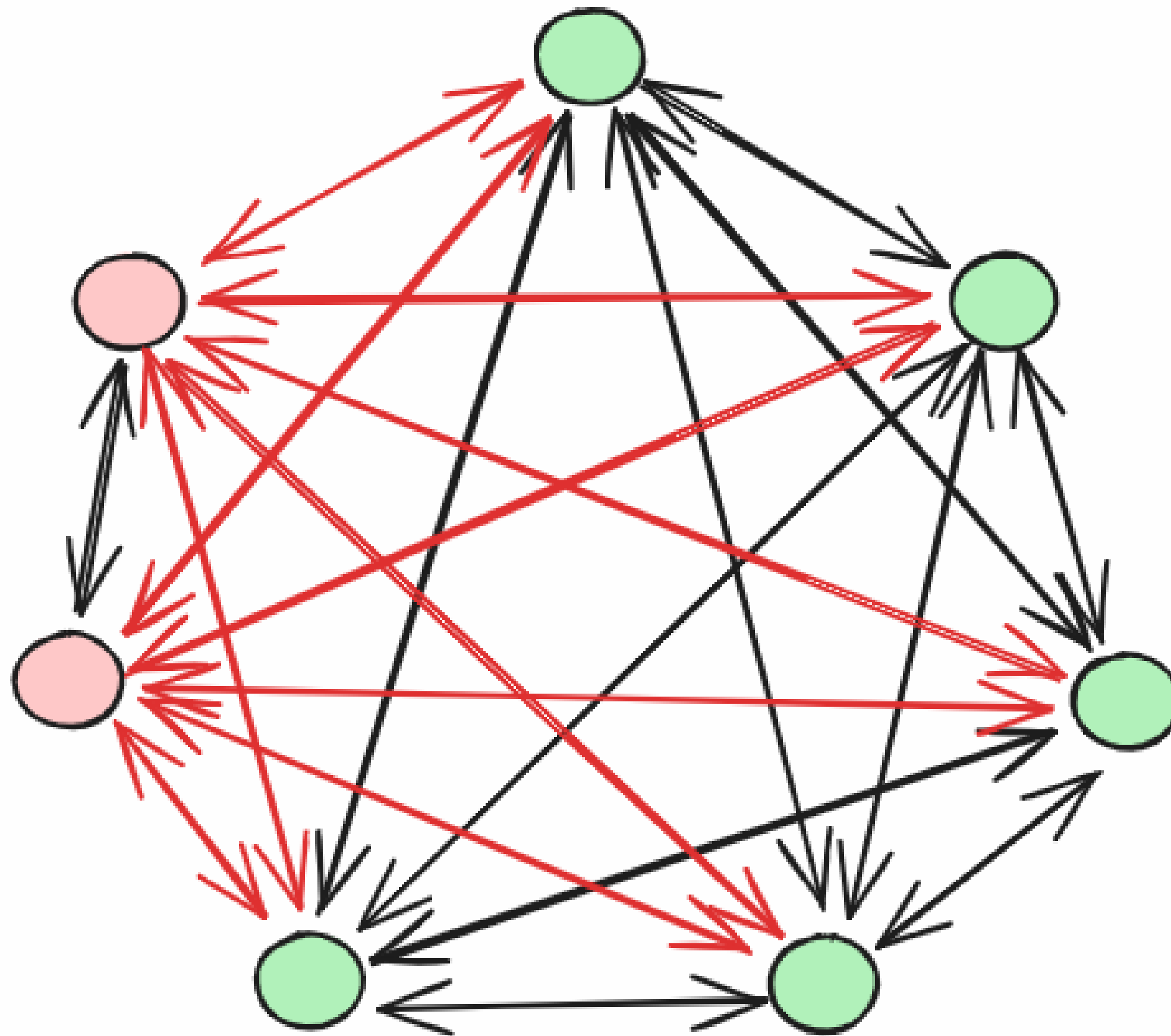
SerNet



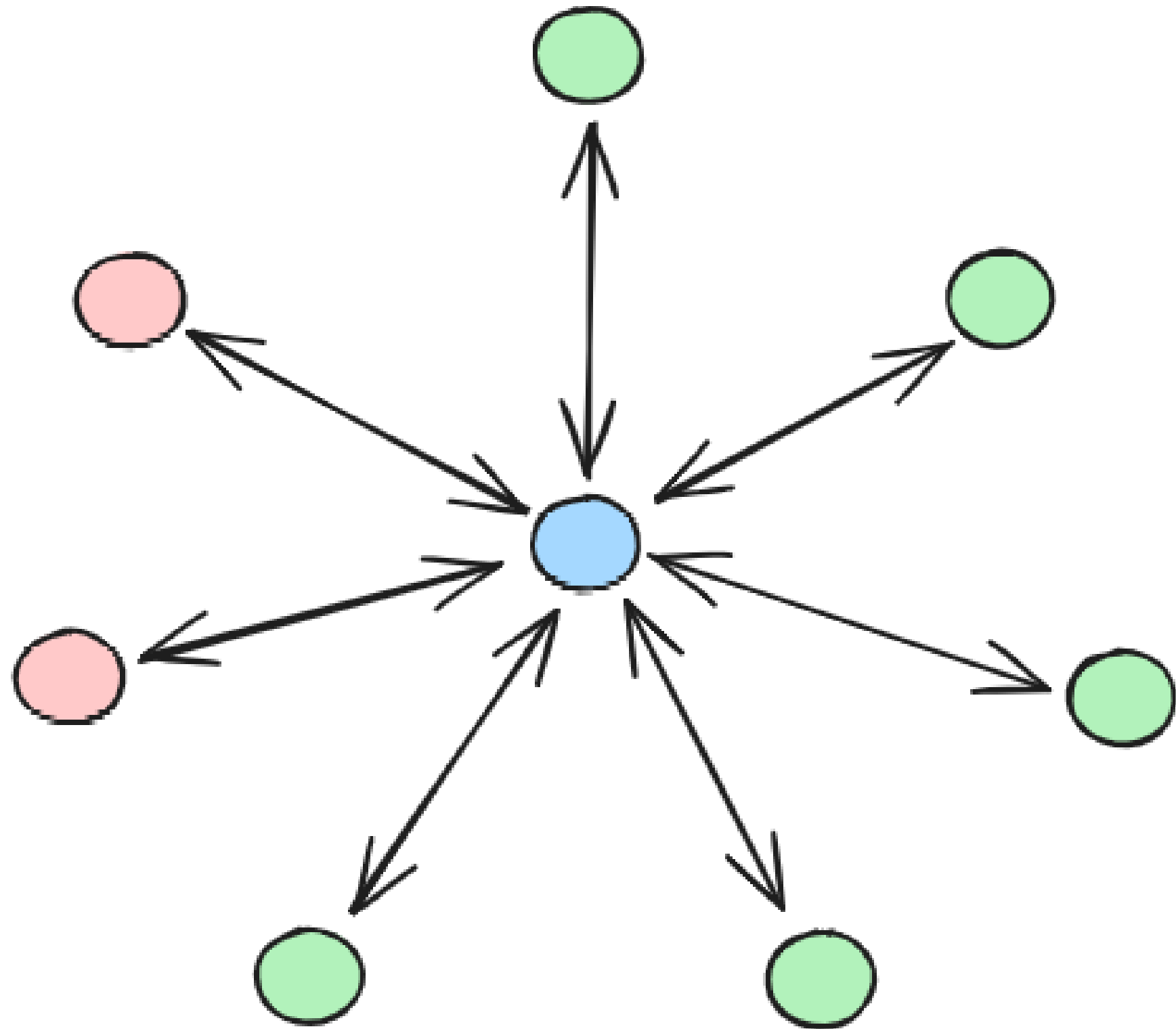
www.sernet.de







$$(7(7-1))/2=21$$



...vs. Hub-Spoke:
7 comm. channels