

Erste Schritte in FACT24 CIM: Die 10 meist gestellten Fragen

F24

Christine Forstmann & Michael Hingerl

Sales & Key Account Manager

20.06.2023 und 04.07.2023

Public



Die 10 meist gestellten Fragen bei der Implementierung von FACT24 CIM

F24

Teil 1 - 20.06.2023:

1. Wie werden die **Action Cards/Checklisten** am besten aufgesetzt?
2. Wie werden die **Phasen** am besten genutzt?
3. Welche Arten von **Reports** sind sinnvoll?
4. Wie werden die **Chats** über den Case Manager am sinnvollsten verwendet?
5. Wofür wird das **Running Log** am besten genutzt?

Teil 2 - 04.07.2023:

6. Was ist "Pflicht" im **Admin Workspace** und was ist "Kür"?
7. Wer sollte **FACT24 CIM User** sein?
8. Welche Tipps gibt es, die integrierte **Karte** zu verwenden?
9. Wie wird ein **Incident erstellt**?
10. Wo findet man **Hilfe**, wenn man nicht mehr weiter weiß?

6.

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME | BERICHT ERSTELLEN | DATEIARCHIV | INCIDENT BOARDS - TAKTISCH

Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine
 Berichtet: 08.05.2023 21:02
 Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung
 Incident-Potenzial: S1

Aktuelle Berichte

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen >

EO | CF | AC

CNN News | Reuters News | RKI | FACT24 | F24 +

Action Cards >

Aufgabenmanagement

Phasen-Tags: Monitoring | Mobilisation | Handling | Normalisation | Evaluation | Andere

Erstanalyse
TAKTISCH 1/5

FORDEC
TAKTISCH 0/6

Krisenstabsleiter
TAKTISCH 1/7

Protokollführer
TAKTISCH 2/7

MOBILISATION
Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase
TAKTISCH 1/9

| Aktion | Verantwortlich | Zugewiesen an | Fälligkeit | Status |
|--|----------------|---------------|------------------|------------------------|
| <input checked="" type="checkbox"/> Vorbewertung Lage > | Notfallmanager | | - | AUSGEFÜHRT |
| <input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab > | Notfallmanager | Eske Ofner | 09.05.2023 10:00 | ALS AUFGABE ZUGEWIESEN |
| <input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe > | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? > | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Dann Abwicklung nach FORDEC > | Notfallmanager | | - | NICHT AUSGEFÜHRT |

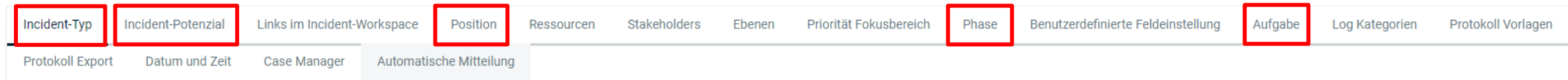
Running Log >

Betreff

- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen > Forstmann, Christine **NICHT GESTARTET**
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab > Ofner, Eske **NICHT GESTARTET**
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen > **AUSGEFÜHRT**
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste >
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke >
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase >
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 >
- INFO** 08.05.2023 21:06 : Meeting aktualisiert >
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents > **AUSGEFÜHRT**
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters > **AUSGEFÜHRT**
- INFO** 08.05.2023 21:05 : Neue Konferenz >
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation > **AUSGEFÜHRT**

6. Was ist “Pflicht” im Admin Workspace und was ist “Kür”?

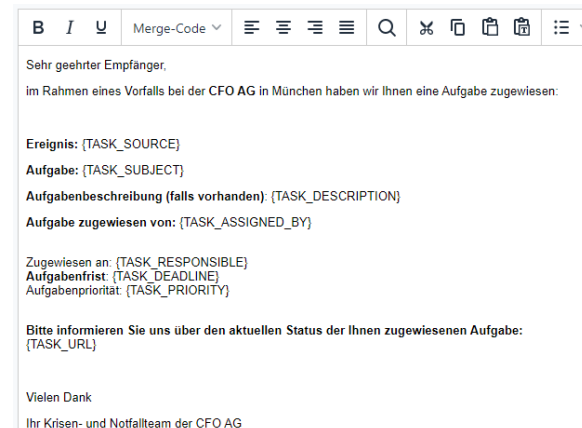
- **Nutzen:** Anpassung an firmenspezifische Nomenklatur und Vorgaben



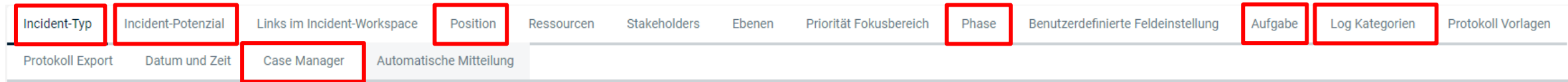
- **MUSS Definitionen = PFLICHT**

- Incident-Typ: Unterscheidung von Vorfallarten
- Incident-Potenzial: Unterscheidung von Schweregraden/Kritikalitäten
TIPP: Hilfreich, wenn bestimmte Aktivitäten erst bei höheren Schweregraden Teil einer Checkliste sind
- Position: Definition von Funktionen/Rollen
- Phase: Definition eines Ordnungskriteriums für Checklisten – siehe Frage 1
- Aufgabe: Personalisierung der Mitteilung im Rahmen der Aufgabenzuweisung

TIPP: FACT24 CIM Daten über MergeCodes einfügen, z.B. Ereignisname als {QUELLE/TASK_SOURCE}



6. Was ist "Pflicht" im Admin Workspace und was ist "Kür"?

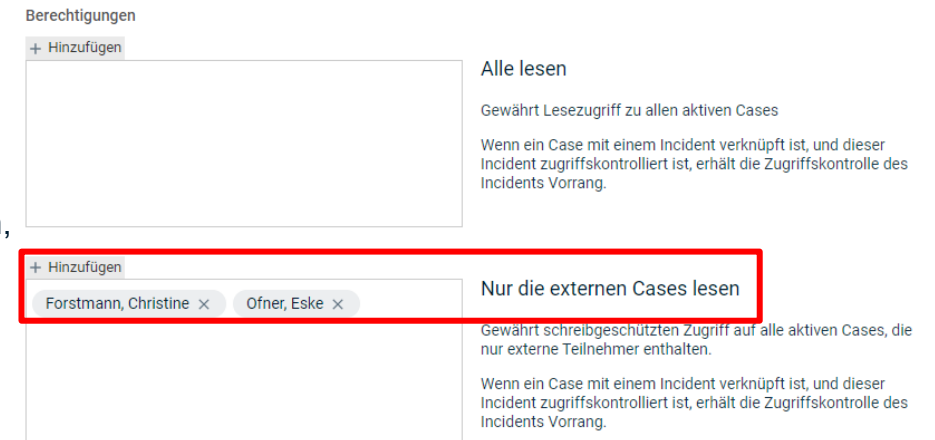


- MUSS Definitionen = PFLICHT**

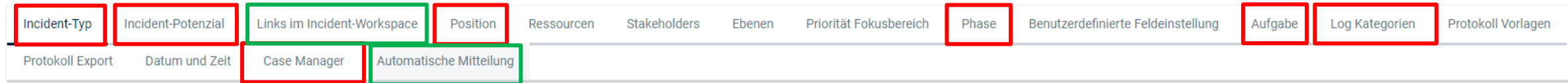
- Log Kategorien: Festlegung von Klassifizierungen und damit späteren Filtermöglichkeiten für Einträge im Running Log und Case Manager Nachrichten
- Case Manager: Festlegung von FACT24 CIM Usern mit Zugriff auf alle Cases

TIPP: mind. 2 CIM Hauptuser für den Zugriff auf die sog. Externen Cases eintragen

„Externe Cases“ sind Cases, die automatisch im Rahmen eines Alarms geöffnet wurden, deren Teilnehmer aber ALLE keine FACT24 CIM User sind. Damit hätte KEINER Zugriff auf diesen Case, um ihn zu bearbeiten, z.B. zu dokumentieren, weitere Teilnehmer einzuladen oder zu schließen.



6. Was ist "Pflicht" im Admin Workspace und was ist "Kür"?



- KANN Definitionen = KÜR
 - Links im Incident-Workspace:** hilfreich für direkten Zugriff auf bestimmte URLs (z.B. Intranet, Gefahrenstoff-Datenbanken, Recherche-Tools)
 - Automatische Mitteilungen:** hilfreich, z.B. für automatische Info an bestimmte Empfänger bei versch. Ereignissen (z.B. Info an Vorstand / Management / Kommunikationsabteilung bei Neuanlage eines Vorfalls eines bestimmten Schweregrades oder bei Veränderung des Schweregrades)



| Automatische Mitteilung | | | | | | | |
|-----------------------------------|---------------------------------------|-------------------------|----------|--------------|-------------|--------------------|----------------------------|
| Titel | Auslöser | Organisation | Ebenen | Incident-Typ | Ereignisort | Incident-Potenzial | Auch im Übungsmodus senden |
| Neues Ereignis - Info an Vorstand | Bei Erstellung des Ereignisses senden | CFO Headquarter München | Taktisch | Alle | | S3 | Nein |

- Home
- Search
- Incident Boards
- Settings
- Navigation arrows
- F24 logo

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 Incident-Potenzial: S1

System 08.05 21:13     

- FACT24 ALARME
- BERICHT ERSTELLEN
- DATEIARCHIV
- INCIDENT BOARDS - TAKTISCH

Incident-Details

Cyberattacke - 8.05.2023

Registriert von Forstmann, Christine
Berichtet 08.05.2023 21:02
Incident-Typ IT Incident / Cyber-Angriffe / Cyber-Bedrohung
Incident-Potenzial S1

Aktuelle Berichte

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.
Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen

- EO
- CF
- AC

- CNN News
- Reuters News
- RKI
- FACT24
- F24



Action Cards

Aufgabenmanagement

- Phasen-Tags:
- Monitoring
 - Mobilisation
 - Handling
 - Normalisation
 - Evaluation
 - Andere

| | | | | |
|--------------|--------------|-------------------|-----------------|--------------|
| Erstanalyse | FORDEC | Krisenstabsleiter | Protokollführer | Mobilisation |
| TAKTISCH 1/5 | TAKTISCH 0/6 | TAKTISCH 1/7 | TAKTISCH 2/7 | TAKTISCH 1/9 |

| Aktion | Verantwortlich | Zugewiesen an | Fälligkeit | Status |
|--|----------------|---------------|------------------|------------------------|
| <input checked="" type="checkbox"/> Vorbewertung Lage | Notfallmanager | | - | AUSGEFÜHRT |
| <input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab | Notfallmanager | Eske Ofner | 09.05.2023 10:00 | ALS AUFGABE ZUGEWIESEN |
| <input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Dann Abwicklung nach FORDEC | Notfallmanager | | - | NICHT AUSGEFÜHRT |

Running Log

- Betreff**
- AUFGABE** 08.05.2023 21:11: Strategische Ebene benachrichtigen (NICHT GESTARTET) - Forstmann, Christine
- AUFGABE** 08.05.2023 21:10: Abstimmung mit dem Management zur vollen Aktivierung Krisenstab (NICHT GESTARTET) - Ofner, Eske
- AKTION** 08.05.2023 21:09: Aktuelle Lage einschätzen (AUSGEFÜHRT)
- ACTION CARD** 08.05.2023 21:09: Taktische Ebene - Checkliste
- ACTION CARD** 08.05.2023 21:09: CFO Europe: Checkliste für die europäischen Werke
- ACTION CARD** 08.05.2023 21:09: Mobilisierungsphase
- BERICHT** 08.05.2023 21:08: Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023
- INFO** 08.05.2023 21:06: Meeting aktualisiert
- AKTION** 08.05.2023 21:06: Aufzeichnung des Incidents (AUSGEFÜHRT)
- AKTION** 08.05.2023 21:06: Unterstützung des Krisenstabsleiters (AUSGEFÜHRT)
- INFO** 08.05.2023 21:05: Neue Konferenz
- INFO** 08.05.2023 21:05: Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04: Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04: Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04: Mobilisierung der internen Krisenorganisation (AUSGEFÜHRT)

7. Wer sollte **FACT24 CIM User** sein?

- **Nutzen:** Alle FACT24 CIM User haben Zugriff auf den Vorfall und haben alle Informationen zur Verfügung
 - Beispiele
 - Kernteam
 - 3-5 Mitarbeiter aus dem Krisenstab
 - 2-3 LogKeeper / Krisenkoordinatoren / Informationsmanager
- Bandbreite
- und alle Schattierungen dazwischen
- Alle Krisenstabsmitglieder und alle Notfallmanager

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME | BERICHT ERSTELLEN | DATEIARCHIV | INCIDENT BOARDS - TAKTISCH

Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine
 Berichtet: 08.05.2023 21:02
 Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung
 Incident-Potenzial: S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.

Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen ▾
 EO CF AC

[CNN News](#) [Reuters News](#) [RKI](#) [FACT24](#) [F24](#) +

Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags: Monitoring Mobilisation Handling Normalisation Evaluation Andere

Erstanalyse
 TAKTISCH 1/5

FORDEC
 TAKTISCH 0/6

Krisenstabsleiter
 TAKTISCH 1/7

Protokollführer
 TAKTISCH 2/7

MOBILISATION
 Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase
 TAKTISCH 1/9

| Aktion | Verantwortlich | Zugewiesen an | Fälligkeit | Status |
|--|----------------|---------------|------------------|------------------------|
| <input checked="" type="checkbox"/> Vorbewertung Lage ▾ | Notfallmanager | | - | AUSGEFÜHRT |
| <input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾ | Notfallmanager | Eske Ofner | 09.05.2023 10:00 | ALS AUFGABE ZUGEWIESEN |
| <input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Dann Abwicklung nach FORDEC ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |

8.



Running Log >

Betreff

- AUFGABE** 08.05.2023 21:11
Strategische Ebene benachrichtigen ▾
Forstmann, Christine NICHT GESTARTET
- AUFGABE** 08.05.2023 21:10
Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾
Ofner, Eske NICHT GESTARTET
- AKTION** 08.05.2023 21:09
Aktuelle Lage einschätzen ▾ AUSGEFÜHRT
- ACTION CARD** 08.05.2023 21:09
Taktische Ebene - Checkliste ▾
- ACTION CARD** 08.05.2023 21:09
CFO Europe: Checkliste für die europäischen Werke ▾
- ACTION CARD** 08.05.2023 21:09
Mobilisierungsphase ▾
- BERICHT** 08.05.2023 21:08
Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 ▾
- INFO** 08.05.2023 21:06
Meeting aktualisiert ▾
- AKTION** 08.05.2023 21:06
Aufzeichnung des Incidents ▾ AUSGEFÜHRT
- AKTION** 08.05.2023 21:06
Unterstützung des Krisenstabsleiters ▾ AUSGEFÜHRT
- INFO** 08.05.2023 21:05
Neue Konferenz ▾
- INFO** 08.05.2023 21:05
Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04
Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04
Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04
Mobilisierung der internen Krisenorganisation ▾ AUSGEFÜHRT

8. Welche Tipps gibt es, die integrierte **Karte** zu verwenden?

- **Nutzen:** unterschätzte visuelle Darstellung von Infos

- **Beispiele**

- Schnelle Lokalisierung von Ressourcen (Mannschaft, Helfer, Fahrzeuge, etc.)



- Kennzeichnung von Details wie gesperrten Straßenzügen oder Eingängen, z.B. bei Demos
Vorteil:

- Leichtere Abstimmung mit der Sicherheitszentrale
- Grundlage für Info an die Mitarbeiter



- ☰
- 🔍
- 🏠
- 📅
- 🗄️
- 👤
- ⚙️
- ➔
- F24

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME BERICHT ERSTELLEN DATEIARCHIV INCIDENT BOARDS - TAKTISCH

Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine
 Berichtet: 08.05.2023 21:02
 Incident-Typ: IT Incident / Cyber-Attacke / Cyber-Bedrohung
 Incident-Potenzial: S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen ▾

EO CF AC

[CNN News](#) [Reuters News](#) [RKI](#) [FACT24](#) [F24](#) +



Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags:

Monitoring Mobilisation Handling Normalisation Evaluation Andere

| | | | | |
|-------------------------------|--------------------------|-------------------------------------|-----------------------------------|---|
| Erstanalyse TAKTISCH 1/5 | FORDEC TAKTISCH 0/6 | Krisenstabsleiter TAKTISCH 1/7 | Protokollführer TAKTISCH 2/7 | Mobilisation Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase TAKTISCH 1/9 |
|-------------------------------|--------------------------|-------------------------------------|-----------------------------------|---|

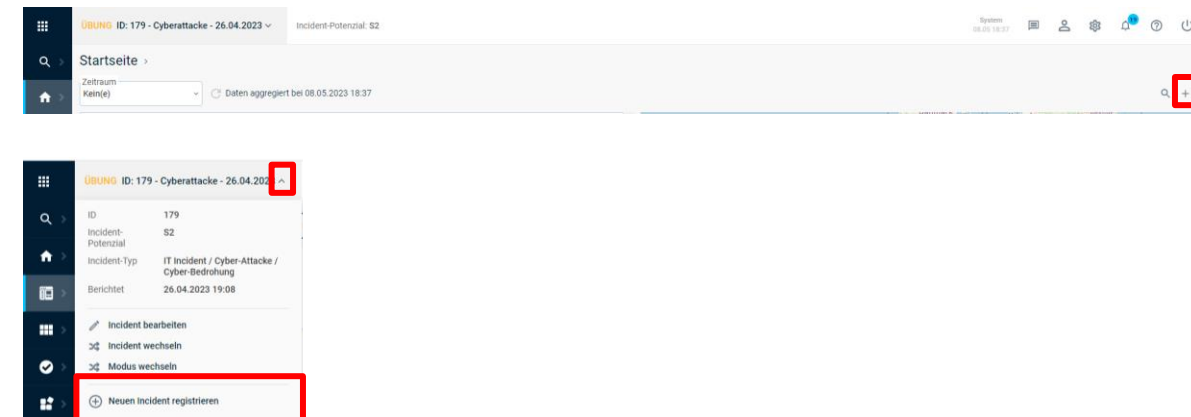
| Aktion | Verantwortlich | Zugewiesen an | Fälligkeit | Status |
|--|----------------|---------------|------------------|------------------------|
| <input checked="" type="checkbox"/> Vorbewertung Lage ▾ | Notfallmanager | | - | AUSGEFÜHRT |
| <input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾ | Notfallmanager | Eske Ofner | 09.05.2023 10:00 | ALS AUFGABE ZUGEWIESEN |
| <input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Dann Abwicklung nach FORDEC ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |

Running Log >

- Betreff**
- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen ▾ Forstmann, Christine NICHT GESTARTET
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾ Ofner, Eske NICHT GESTARTET
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen ▾ AUSGEFÜHRT
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste ▾
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke ▾
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase ▾
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 ▾
- INFO** 08.05.2023 21:06 : Meeting aktualisiert ▾
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents ▾ AUSGEFÜHRT
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters ▾ AUSGEFÜHRT
- INFO** 08.05.2023 21:05 : Neue Konferenz ▾
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation ▾ AUSGEFÜHRT

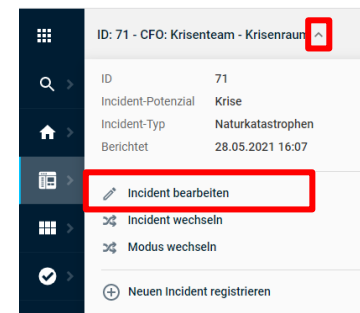
9. Wie wird ein **Incident erstellt** ?

- **Nutzen:** Je nach internem Prozess bestehen mehrere Möglichkeiten, einen neuen Incident zu erstellen
- **Manuelle** Erstellung
 - **Beispielsituation**
 - Das Kernteam hat eine erste Telefonkonferenz durchgeführt, um die ersten Informationen auszutauschen
 - Es wird beschlossen, FACT24 CIM für die Bewältigung einzusetzen
 - Die Verantwortung für die Erstellung des Incidents obliegt einer bestimmten Rolle und wird manuell durchgeführt
 - **Wege** der manuellen Erstellung
 - „+“-Menü auf der Startseite
 - Drop Down-Menü neben dem Namen des Incidents, der gerade bearbeitet wird



9. Wie wird ein **Incident erstellt** ?

- **Automatische Erstellung**
 - **Beispielsituation**
 - Das Kernteam hat eine erste Telefonkonferenz durchgeführt, um die ersten Informationen auszutauschen
 - Es wird beschlossen, FACT24 CIM für die Bewältigung einzusetzen
 - Incidents werden dabei automatisch erstellt
 - **WICHTIG:**
 - Incidents, die automatisch über einen Alarm erstellt werden, sind immer im „**Normal**“ Modus registriert und haben standardmäßig den Namen des Alarms
 - Der Name des Incidents, der Incidenttyp, der Schweregrad, die Karte etc. können im Nachgang noch bearbeitet und verändert werden
 - Drop Down-Menü neben dem Namen des Incidents



9. Wie wird ein **Incident erstellt** ?

- **Wege** der automatischen Erstellung
 - Bei **Auslösung eines FACT24 Alarms** wird ein neuer Incident erstellt
 - **Vorab implementiert** in den Grundeinstellungen des Alarms

FACT24 ENS F24

CFD Headquarter München (10999) Christine Forstmann Abmelden

CFD Headquarter München

Deutsch

Home Administration Operating Setup Enterprise

« ZURÜCK

Alarm: (1000) - CFO: Krisenteam - Krisenraum

Grundeinstellungen Weitere Einstellungen Meldungen Aufforderung zur Eingabe der Rückmeldung Gruppen Berichts-Endgeräte

Nummer 1000

Bezeichnung CFO: Krisenteam - Krisenraum

Konferenz Nein

Alarmaktivierer in die Konferenz einbeziehen Nein

Einen Incident in FACT24 CIM registrieren Ja

Incident-Typ

Markt- oder finanzwirtschaftliche Herausforderung Auswirkungen hinsichtlich Reputation Terroranschlag Andere

Vorsätzliche Handlungen Gebäudeausfall Pandemie Brand

Stoffaustritt Personenschaden Infrastrukturausfälle IT Incident / Cyber-Angriff / Cyber-Bedrohung

RZ Ausfall Naturkatastrophen

Incident-Potenzial SI

Incident-Phase

Einen Case in FACT24 CIM öffnen Nein

Probearm Nein

Benachrichtigungsraum

F24 push notification Ton Alarmton

Neuer Alarm

zuletzt bearbeitet von UserName932001, 08.05.23 16:15:05

9. Wie wird ein **Incident erstellt** ?

- **Adhoc Erstellung** beim Auslösen eines FACT24 Alarms

The screenshot shows the FACT24 ENS F24 interface. The navigation menu includes Home, Administration, **Operating**, Setup, and Enterprise. A progress bar at the top indicates six steps: 1. Gruppenzuordnung ändern, 2. Zusätzliche Personen zuordnen, 3. Endgeräte ändern, 4. Raum öffnen, 5. **Incident registrieren**, and 6. Alarm starten. Below the progress bar, the activation details are shown: 'Aktivierung: Alarm 1000 CFO: Krisenteam - Krisenraum'. A checkbox labeled 'Für diesen Alarm einen Incident in FACT24 CIM registrieren.' is checked and highlighted with a red box. Below this, there are dropdown menus for 'Incident-Phase' and 'Incident-Potenzial *'. To the right, there is a list of 'Incident-Typ *' options, including Brand, Stoffaustritt, RZ Ausfall, Gebäudeausfall, Infrastrukturausfälle, IT Incident / Cyber-Angriffe / Cyber-Bedrohung, Markt- oder finanzwirtschaftliche Herausforderung, Naturkatastrophen, Terroranschlag, Pandemie, Personenschaden, Auswirkungen hinsichtlich Reputation, Vorsätzliche Handlungen, and Andere. At the bottom left, there is a checkbox for 'Einen Case in FACT24 CIM öffnen'. The footer contains 'F24 AG © 2023 Datenschutz FACT24' and '2.29.0.5 Edition: FACT24 CIM advanced'.

- **Automatische Erstellung** eines Incidents über ein **externes Tool**
Ab FACT24 CIM essential gibt es eine Webservice API, die zur automatischen Erstellung eines Incidents aus einem Drittsystem (z.B. Ticketing-/Monitoring Tool) genutzt werden kann

-
-
-
-
-
-
-
-
-
- F24**

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

System 08.05 21:13

- FACT24 ALARME
- BERICHT ERSTELLEN
- DATEIARCHIV
- INCIDENT BOARDS - TAKTISCH

Incident-Details >

Cyberattacke - 8.05.2023

Registriert von Forstmann, Christine
 Berichtet 08.05.2023 21:02
 Incident-Typ IT Incident / Cyber-Angriffe / Cyber-Bedrohung
 Incident-Potenzial S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen ▾

- EO
- CF
- AC

- CNN News
- Reuters News
- RKI
- FACT24
- F24
- +



Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags:

- Monitoring
- Mobilisation
- Handling
- Normalisation
- Evaluation
- Andere

Erstanalyse 1/5

TAKTISCH

FORDEC 0/6

TAKTISCH

Krisenstabsleiter 1/7

TAKTISCH

Protokollführer 2/7

TAKTISCH

Mobilisation 1/9

TAKTISCH

Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase

| Aktion | Verantwortlich | Zugewiesen an | Fälligkeit | Status |
|--|----------------|---------------|------------------|------------------------|
| <input checked="" type="checkbox"/> Vorbewertung Lage ▾ | Notfallmanager | | - | AUSGEFÜHRT |
| <input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾ | Notfallmanager | Eske Ofner | 09.05.2023 10:00 | ALS AUFGABE ZUGEWIESEN |
| <input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |
| <input type="checkbox"/> Dann Abwicklung nach FORDEC ▾ | Notfallmanager | | - | NICHT AUSGEFÜHRT |

Running Log >

- Betreff**
- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen ▾
Forstmann, Christine NICHT GESTARTET
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾
Ofner, Eske NICHT GESTARTET
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen ▾ AUSGEFÜHRT
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste ▾
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke ▾
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase ▾
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 ▾
- INFO** 08.05.2023 21:06 : Meeting aktualisiert ▾
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents ▾ AUSGEFÜHRT
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters ▾ AUSGEFÜHRT
- INFO** 08.05.2023 21:05 : Neue Konferenz ▾
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation ▾ AUSGEFÜHRT

10. Wo findet man **Hilfe**, wenn man nicht mehr weiter weiß?

- **Nutzen:** Hilfe zur Selbsthilfe 😊

- Hilfeseite in FACT24 CIM



- Hilfeportal für FACT24 mit vielen CIM Themen <https://help.fact24.com/l/de>

- **TIPP:**

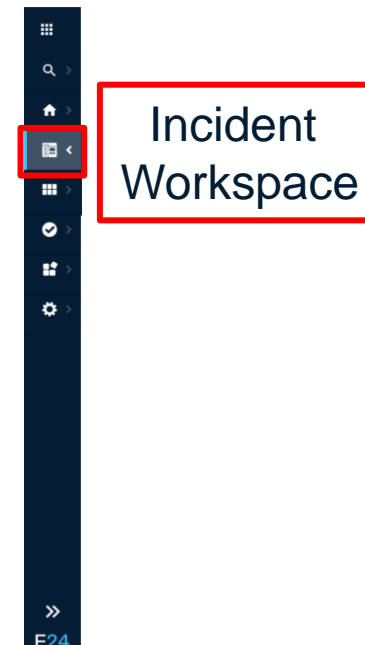
- Zugriff auf den aktuell bearbeiteten Vorfall erhält man immer über den sog. **Incident Workspace** in der linken Menüleiste = zentraler Ausgangspunkt für die Bearbeitung des Vorfalls

- Ausschau halten nach

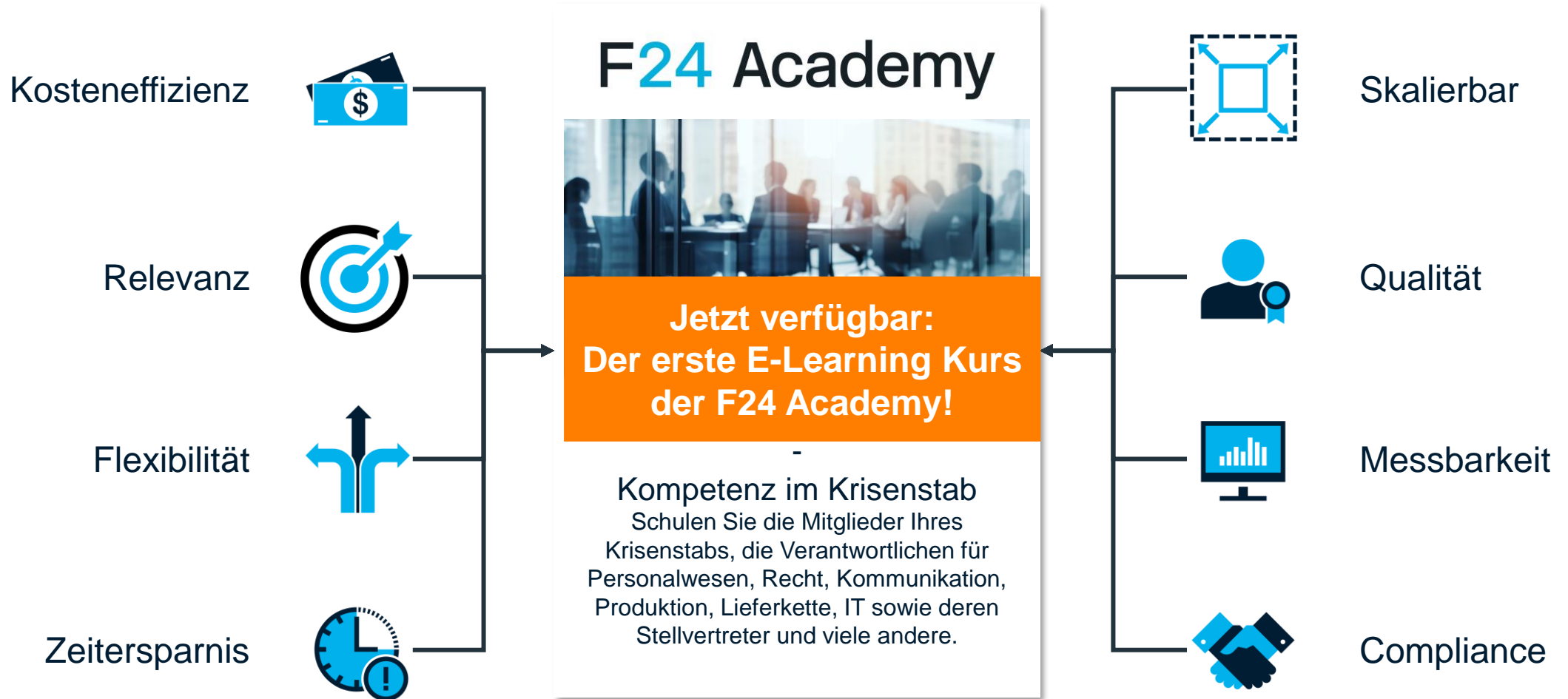
- dem „3-Punkte“ Menü in **jedem** Bereich



- Dem „+“ – Zeichen in **jedem** Bereich



Stellen Sie Ihr Krisenmanagement auf eine solide Basis!



Vielen Dank für Ihre Aufmerksamkeit!

F24



Rechtlicher Hinweis

F24



Diese Inhalte unterliegen dem Schutz durch das Urheberrecht. Jede von anwendbarem Urheberrecht nicht zugelassene Verwertung erfordert die vorherige ausdrückliche und schriftliche Zustimmung des Rechtsinhabers. Hiervon berührt sind insbesondere das Recht zur Vervielfältigung, Übersetzung, Bearbeitung, Einspeicherung, Verbreitung bzw. Widergabe in Datenbanken oder andere elektronische Systeme und Medien. Jede urheberrechtlich oder durch den Rechtsinhaber nicht ausdrücklich zugelassene Verwertung ist unzulässig und ggfs. strafbar.