RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Lieferobjekte RAILplus

Livrables RAILplus

Cyber Day

10.06.2024
Aarau

Agenda - Die Cyberreise der RAILplus Bahnen
Agenda – Le voyage cyber des CFs RAILplus

- Woher kommen wir?
  D’où venons-nous?

- Was war der Weg bis heute?
  Quel fût le chemin jusqu’à ajd?

- Wohin wir demnächst gehen?
  Où allons-nous prochainement?

Woher kommen wir?
D'où venons-nous?

Cyberbedrohungen und Risiken wachsen

Les menaces et risques cyber grandissent

Herausforderungen in Bezug auf Fähigkeiten und Mittel

Défis en termes de compétences et de moyens

RAILplus der ideale Kooperationspartner

RAILplus le partenaire idéal pour la coopération

Synergien durch RAILplus / Synergies grâce à RAILplus

Überblick der Aktivitäten | Aperçu des activités

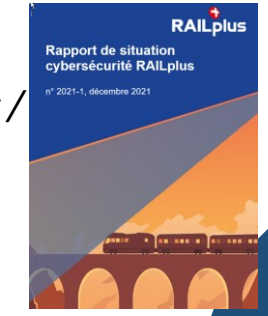
Auswertung der Maturität / Évaluation de la maturité

2020

Kick-off und Assessment der Cybersicherheit
Coup d'envoi et évaluation de la cybersécurité

2021

Lagebericht / Rapport de situation



SWISSRAIL Industry Association

BAV /OFT

SBB / CFF

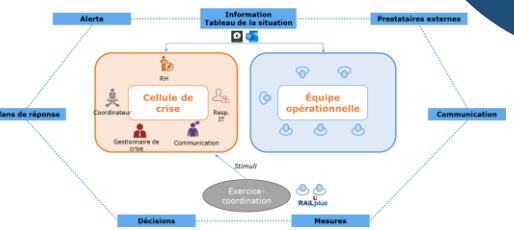
NCSC / BACS

8 Massnahmen: Detektion, Vertragsanhang, Austausch, ..
8 mesures : outil de détection, annexe au contrat, échanges,…

Lerneinheit E-Learning / Module d'e-learning

2022

4 Massnahmen: ISMS, Sensibilisierung, OT-Sicherheit, Cyberkrise
4 mesures : ISMS, sensibilisation, sécurité OT, exos crises cyber



Cyberkrisen Übung / Exercice de crise cyber

2023

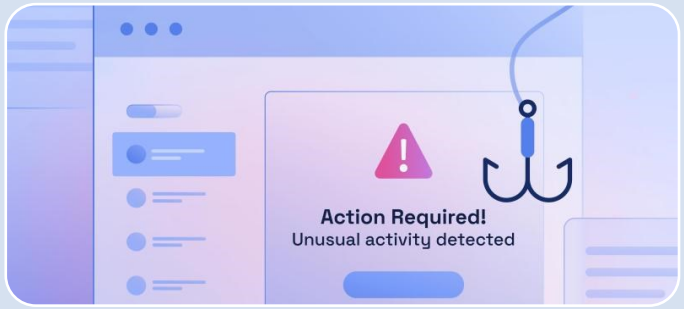
3 Massnahmen : Umsetzung ISMS, IR Playbooks, MS365 Sicherheit
3 mesures : Implémentation ISMS, playbooks IR, sécurité MS365

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Fokus auf Aktivitäten und Lieferobjekte

Focus sur les activités et livrables

Sensibilisierung und Ausbildung
Sensibilisation et Formations



Social Engineering und Phishing Training

Training pour prévenir l'ingénieurie sociale et le phishing

E-Learning Plattform Moodle

E-Learning plateforme Moodle

Präsenzschulungen

Formations en présentiel

Cyber Security Baseline als Auftrags-/ Vertragsbestandteil

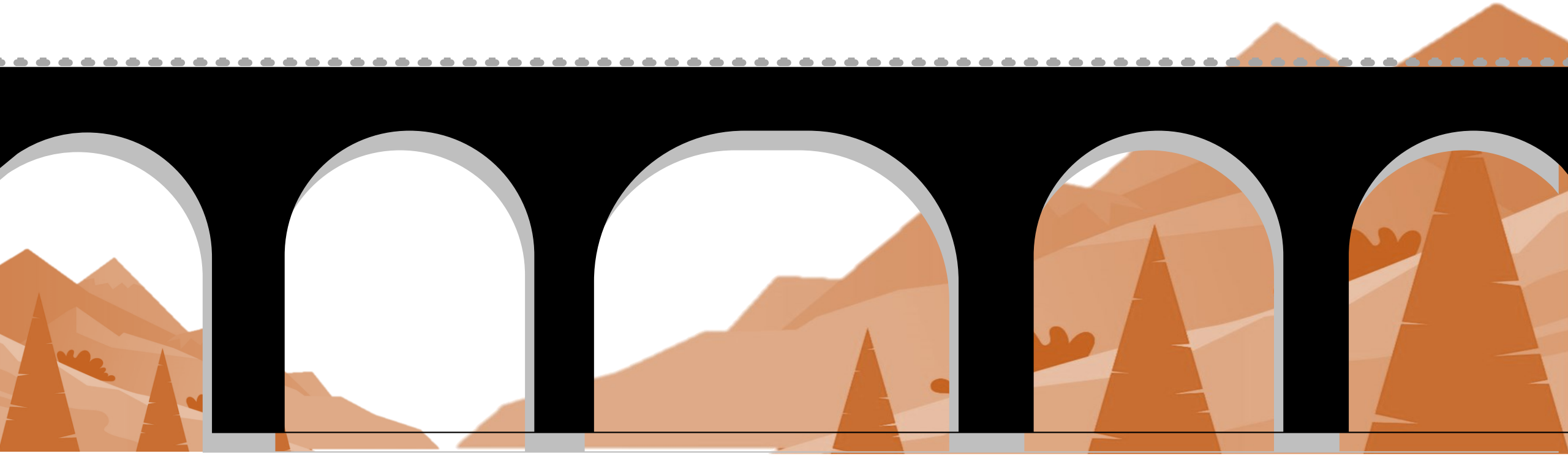
- Anforderungen dienen als Orientierungshilfe für die Bahnen und besitzen Grundschutzcharakter

- Die Anforderungen dienen lediglich als Vorschlag und können durch die Mitgliederbahnen angepasst werden

Inhaltsverzeichnis

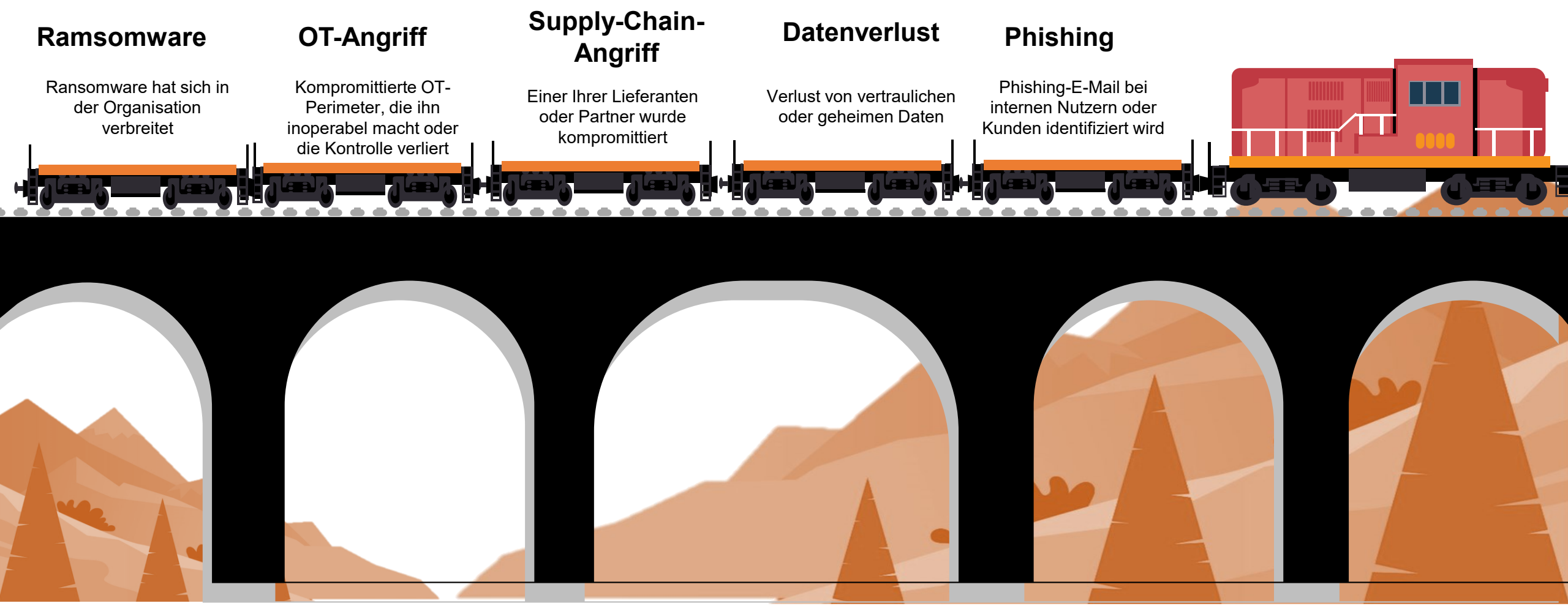
Playbooks

Ein Playbook enthält klare und eindeutige Anweisungen für den Reaktion auf einen (Cyber-)Vorfall.
Un playbook fournit de instructions claires et précisent pour faire face à un incident (cyber)



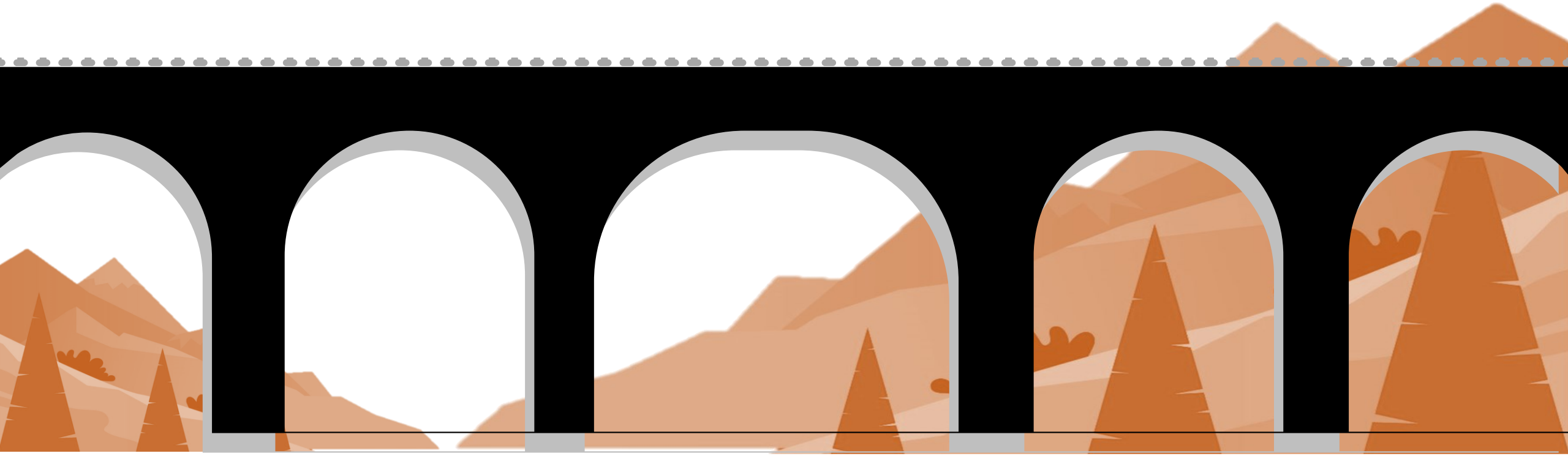
Playbooks

Ein Playbook enthält klare und eindeutige Anweisungen für den Reaktion auf einen (Cyber-)Vorfall.
Un playbook fournit de instructions claires et précisent pour faire face à un incident (cyber)

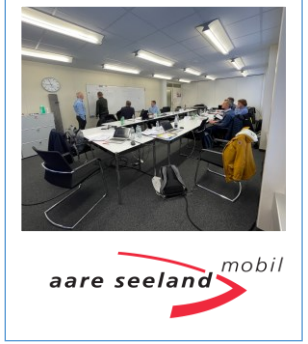


Playbooks

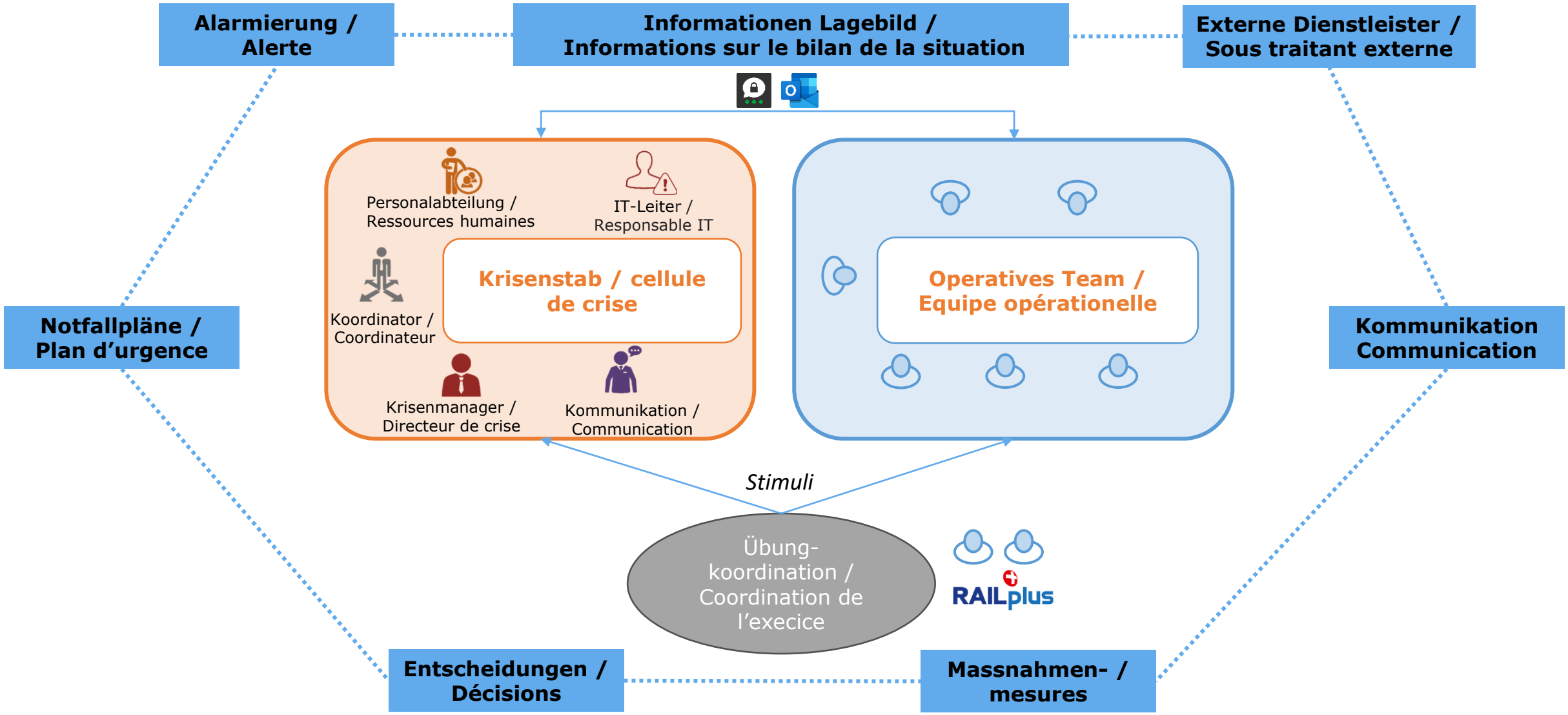
Ein Playbook enthält klare und eindeutige Anweisungen für den Reaktion auf einen (Cyber-)Vorfall.
Un playbook fournit de instructions claires et précisent pour faire face à un incident (cyber)



Cyberkrise-Übungen | Exercices de crise cyber



Cyberkrise Übung | Exercice de crise cyber



Die wichtigsten Schritte zur Detektion von Bedrohungen in IT und OT

Welt der IT | Welt der OT

0 Vor der Einführung von Erkennungslösungen muss eine gute Sicherheitshygiene implementiert werden, um Eindringlinge so weit wie möglich einzuschränken: Inventarisierung der Assets, Netzwerksegregation, Deaktivierung jeglicher nicht nützlicher Software oder Zugänge, Anwendung des Prinzips der geringsten Privilegien auf alle internen Benutzer und Dienstleister usw.

1 **Sensibilisierung der Nutzer für bösartige Bedrohungen und Verhaltensweisen** : Schulungen, gezielte Sensibilisierungskampagnen (Phishing, Präsidentenbetrug), Tischübungen und Simulation von Cyberkrisen.

2 **Identifizieren Sie einen SPOC, der sich mit der Erkennung und Bearbeitung von Sicherheitswarnungen befasst:** eine Person aus der IT, die für die Bearbeitung von Sicherheitsvorfällen verantwortlich ist (Hauptkontakt, Verbindung zum Management, Verbindung zu 3rd Party, Überwachung der Bearbeitung von Vorfällen).

3 **Einführung einer Protokollierungspolitik:** Bei Verdacht auf einen Vorfall oder böswilliges Verhalten müssen die Protokolle aufbewahrt und für manuelle Untersuchungen zugänglich gemacht werden können.

4 **Überwachung des Zugriffs über Remote Access-Lösungen (M2):** Granulare Kontrolle des Zugriffs auf Infrastrukturen und Anwendungen, Einrichtung von Warnmeldungen bei verdächtigen Verbindungen.

5 **Implementieren einer Lösung auf Netzwerkebene, um Eindringlinge zu erkennen und/oder zu verhindern (je nach verwendeten Protokollen):** IDS/IPS oder Einrichten eines Honeypots, um den Angreifer zu täuschen

IDS: Sonden zur Analyse und zum Vergleich des Netzwerkverkehrs auf der Grundlage bekannter Netzwerkangriffe
IPS: Vergleichssonden und Blockierung von Netzwerkpaketen entsprechend den implementierten Sicherheitsprofilen

IDS: Sonden, die den Netzwerkverkehr (ausschliesslich Ethernet-Protokoll) analysieren und vergleichen, um nicht legitime Protokolle zu identifizieren und eine Warnung zu senden (z. B. DHCP- oder DNS-Verbindungen).

Passive Sonden anwenden, um Störungen im Netzwerk zu vermeiden

6 **Regelmässige Scans auf Schwachstellen und Entdeckungen durchführen:** Identifizierung der zu scannenden Quellen, Scannen der Schwachstellen, Behandlung der Schwachstellen über Sanierungspläne . ⚠ OT: Scans können sich negativ auf den Betrieb von Assets auswirken.

7 **Aktivieren Sie eine EDR-Lösung vom Typ "Microsoft Defender": Eine** IT-Erkennungslösung, die nativ auf den Rechnern vorhanden und kostengünstig ist (~5 CHF/Monat).

8 **Eine SIEM-ähnliche Lösung verwenden:** Sammlung und Verwaltung von Logs, Korrelation von Ereignissen und Generierung von Warnmeldungen (gemanagtes oder nicht gemanagtes Angebot).

9 **Verwenden Sie eine Threat-Intelligence-Lösung:** eine fortschrittliche Lösung mit einer Engine für künstliche Intelligenz, die bösartige Verhaltensweisen erkennt und blockiert und dabei selbstständig lernt.

ISMS-Konzept

Leichteres und relevantes ISMS-Konzept für RAILplus-Mitglieder (basierend auf ISO 27001 / ISO 27002), das **sowohl IT als auch OT** behandelt, auf der Grundlage der Anforderung der AB-EBV

Auswahl von Kontrollen und Unterkontrollen

- **4 Themenbereiche**
  - Individuen,
  - Physik,
  - Organisation,
  - Technologien
- Auswahl der **wesentlichsten** Kontrolle und Unterkontrolle für RAILplus-Mitglieder
- **Detaillierte und kontextbezogene** Erklärungen der Kontrolle und Unterkontrolle für OT und IT

Tipps zur Umsetzung

Für jede Kontrolle und Unterkontrolle :

- Schätzung des **Arbeitsaufwands** und des **Budgets** bei der Umsetzung.
- Vorschlag für eine **Prioritätsstufe**

➔ Trotzdem sind die Schätzungen von den Eisenbahnen unter Berücksichtigung **der bereits vorhandenen Situation** anzupassen

2-Tage Unterstützung

- Jede Bahn bekommt **zwei Tage Support** vom RAILplus Kompetenzzentrum für Cybersicherheit
- Damit können die Bahnen ein Feedback über seine Umsetzungspläne oder Hilfe bei Aufbau von bestimmten Massnahmen

Les mesures
Die Kontrollen

Kontrolle

Sicherheit von Assets vor Ort

Unterkontrollen

Mit der Kontrolle verbunden "Sicherheit von Assets vor Ort"

4.3.5 Sicherheit von Assets vor Ort

Implementierungspriorität und Aufwand		Reife bei der Bewertung 2020 (RAILplus Durchschnitt)	
IT	OT	IT	OT
P1	P1	2.1/4	
OPEX	L		
CAPEX	M		

Die Assets vor Ort (Server, Arbeitsstationen, Automaten usw.) müssen geschützt werden, um Schäden, Diebstähle und Kompromittierungen zu vermeiden, die zu Ausfallzeiten und/oder Integritätsverlusten führen können, die für die Organisation von entscheidender Bedeutung sind:

- [P1][S][S] Das Befolgen von Empfehlungen von Herausgebern/Lieferanten bezüglich der physischen Sicherheit von Geräten insbesondere bei Automaten.
- [P1][S][-] Geräte (einschliesslich eines Arbeitsplatzes oder Speichermediums) nicht unbeaufsichtigt und ungesichert an einem öffentlichen Ort zurück lassen.
- [P1][M][S] Das Pflegen von einem aktuellen Inventar der Assets, inklusive Eigentümer und einer Liste der Personen mit Zugang zu diesen.
- [P1][M][S] Verfolgung von Ausrüstungen, die den Standort verlassen sollen, und Einrichtung eines speziellen Genehmigungsverfahrens je nach Kritikalität der Ausrüstung (durch ein Management validierter Antrag).

Weitere Synergien

- Veranstaltungen wie heute
- Des événements tels qu'aujourd'hui

- Antworten auf Vernehmlassungen, wie z.B. zur Meldepflicht von Cyberangriffen
- Des réponses à des consultations, tel que pour l'obligation d'annonce des attaque cyber

RAILplus
Die Meterspurigen
La voie métrique
A scartamento metrico

Wohin wir demnächst gehen?

Où allons-nous prochainement?

Massnahmen 2024
Mesures 2024

- Die Arbeit geht mit weiteren Massnahmen fort:
  - ISMS
  - Zusammenarbeit mit der Industrie
  - SOC / Sicherheitsüberwachung

- Le travail se poursuit avec d'autres mesures :
  - ISMS
  - Collaboration avec l'industrie
  - SOC / surveillance de la sécurité

Workshops heute Nachmittag
Ateliers cet après-midi

Workshop 1: Risiken / Risques

Austausch über Cyberrisiken, die die Eisenbahn betreffen, unabhängig von der Abteilung oder Ebene

Echange sur les risques cyber qui touchent les chemins de fer, quel que soit le département ou l'échelon

Workshop 2: Herausforderungen zur Erhöhung der Cybersicherheit

Défis à relever pour améliorer la cybersécurité

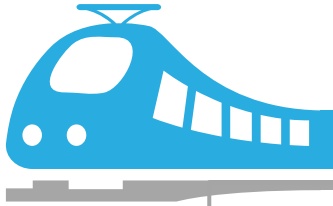
Austausch über die Herausforderungen, denen sich die Eisenbahnen bei der Verbesserung der Sicherheit gegenübersehen

Echange sur les défis auxquels les chemins de fer font face pour améliorer la sécurité

- Wir teilen uns in 4 Gruppen (2x FR, 2x DE)
- Nous nous divisons en 4 groupes (2x FR, 2x DE)

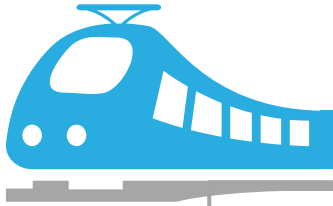
- Jeder Teilnehmer nimmt an beide Workshops
- Chaque participant participe aux deux ateliers

Gemeinsam sind wir stärker | Unis, nous sommes plus forts



Das Cybersicherheitszentrum von RAILplus steht jedem TU zur Verfügung

- Zugriff auf alle bestehende und künftige Lieferobjekte und Dienstleistungen
- Austausch mit anderen Firmen und Stellen wie BAV, SwissRAIL, SBB oder NCSC/BACS
- Günstig durch Skalierbarkeit



Le centre de cybersécurité de RAILplus est à la disposition de chaque ET

- Accès à tous les objets de livraison et services existants et futurs
- Échange avec d'autres entreprises et services tels que l'OFT, SwissRAIL, CFF ou le NCSC
- Avantageux grâce à l'effet d'échelle