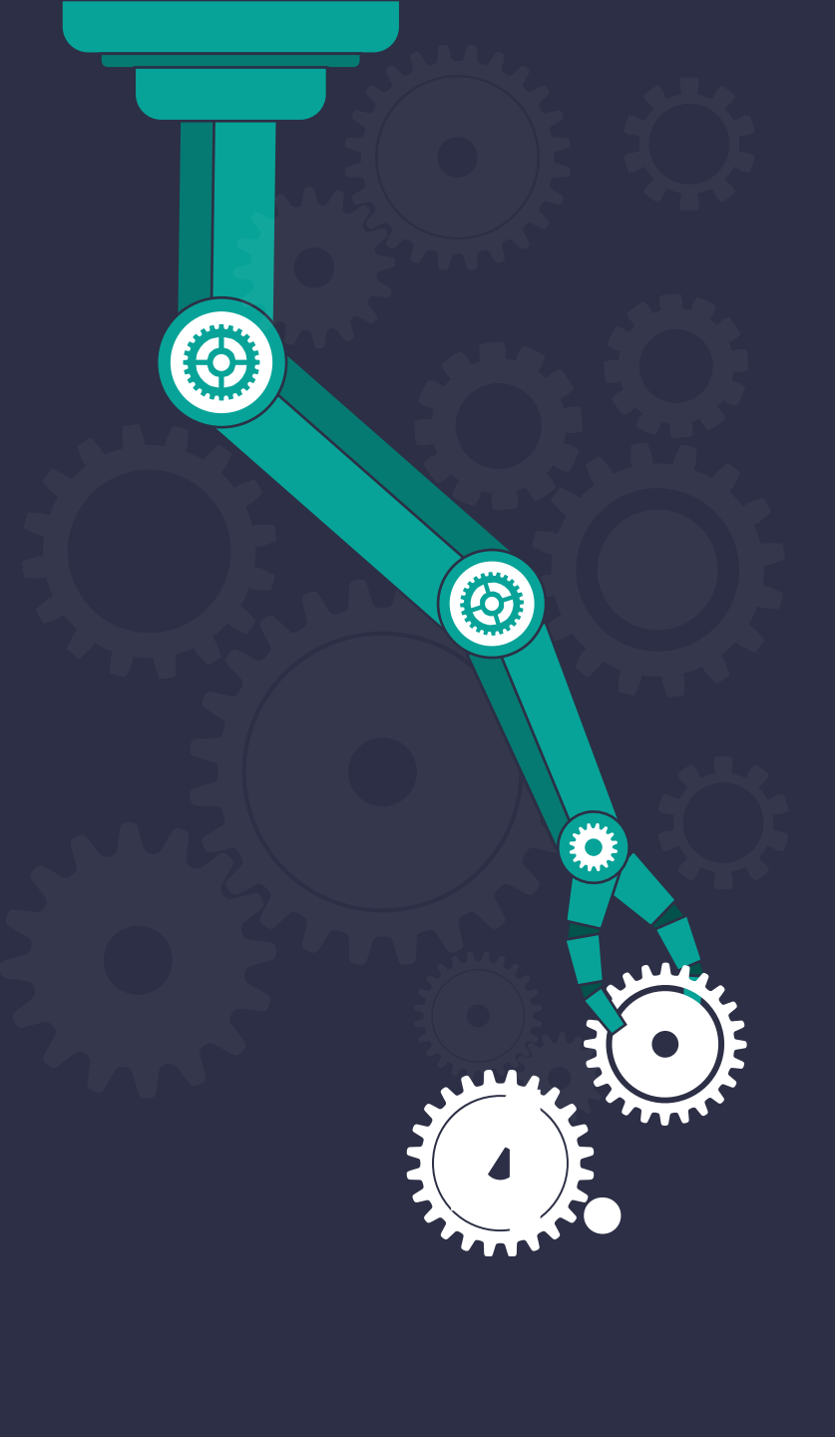
Cybersecurity & Supply Chain Risk Management

Vincenzo Calabrò



Agenda

- Cos’è un Supply Chain Attacks?
- I Vettori di Attacco e Settori Target
- Perchè Supply Chain Risk Management è importante?
- Valutazione dei rischi per la sicurezza informatica
- Valutazione del rischio del fornitore
- I Framework del Supply Chain Risk
- Valutazione del rischio del fornitore
- Gestione delle relazioni con i fornitori
- Implementazione di strategie di approvvigionamento efficaci

Cos’è un Supply Chain Attack?

Gli attacchi alla catena di fornitura sono una minaccia emergente che prende di mira sviluppatori e fornitori di software.

L'obiettivo è accedere ai codici sorgente, creare processi o aggiornare meccanismi infettando app legittime per distribuire malware.

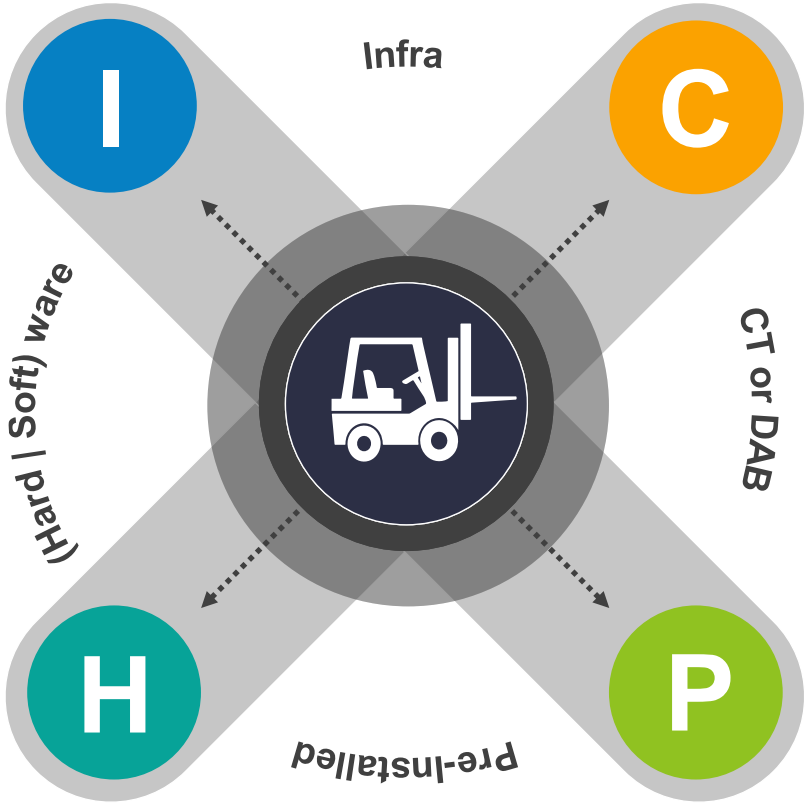
Vettori di Attacco

Compromissione della creazione o aggiornamento dell'infrastruttura

Gli aggressori compromettono gli strumenti di creazione del software o aggiornano l'infrastruttura.

Compromissione dell’hardware o del software

Gli aggressori compromettono il codice specializzato incorporato nei componenti hardware o firmware.

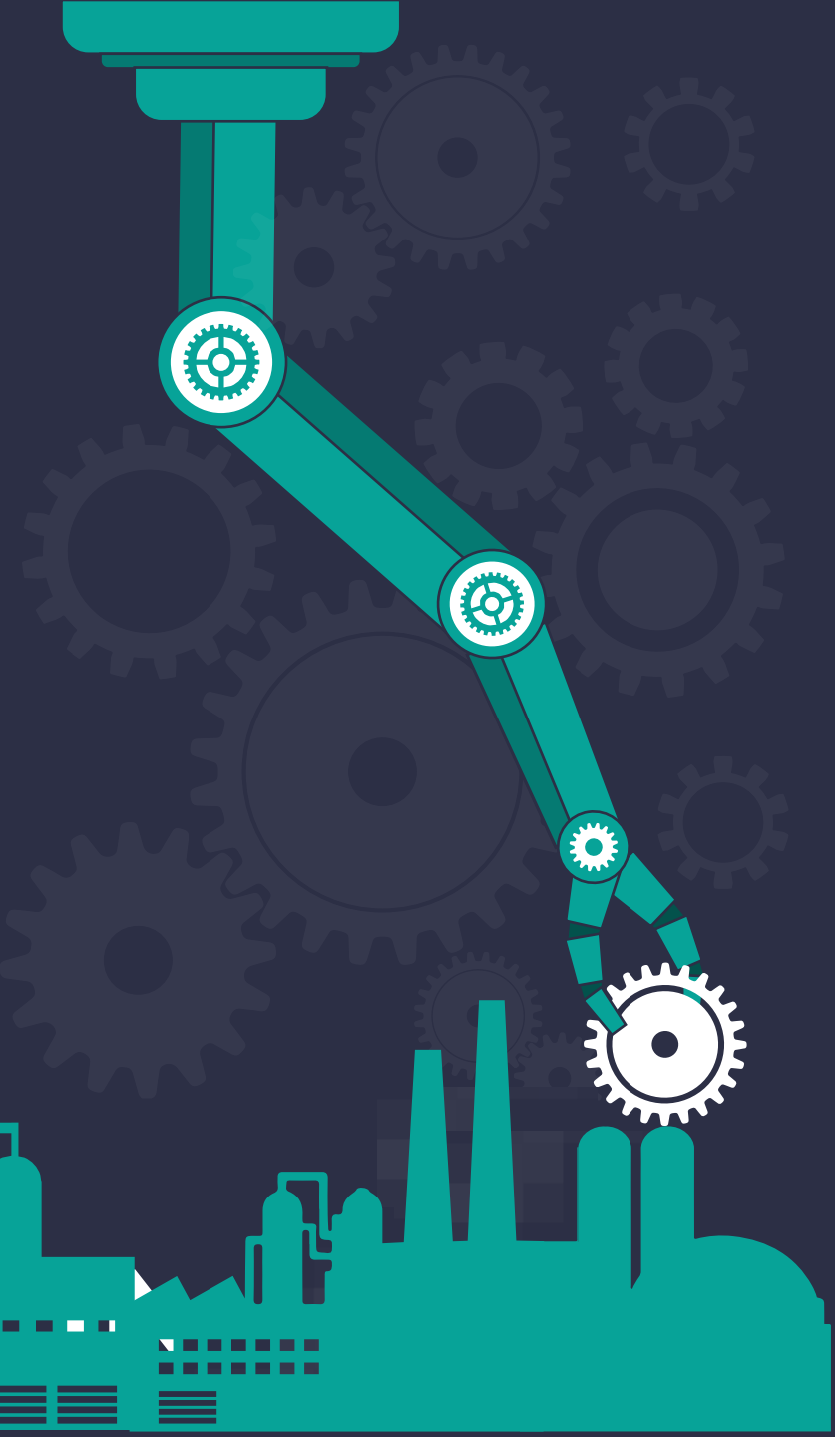


Furto dei certificati o violazione dell'account di sviluppatore

Gli aggressori rubano i certificati di firma del codice o utilizzano account sviluppatore compromessi per firmare applicazioni dannose con l'identità dell'azienda sviluppatrice.

Malware preinstallato nel dispositivo

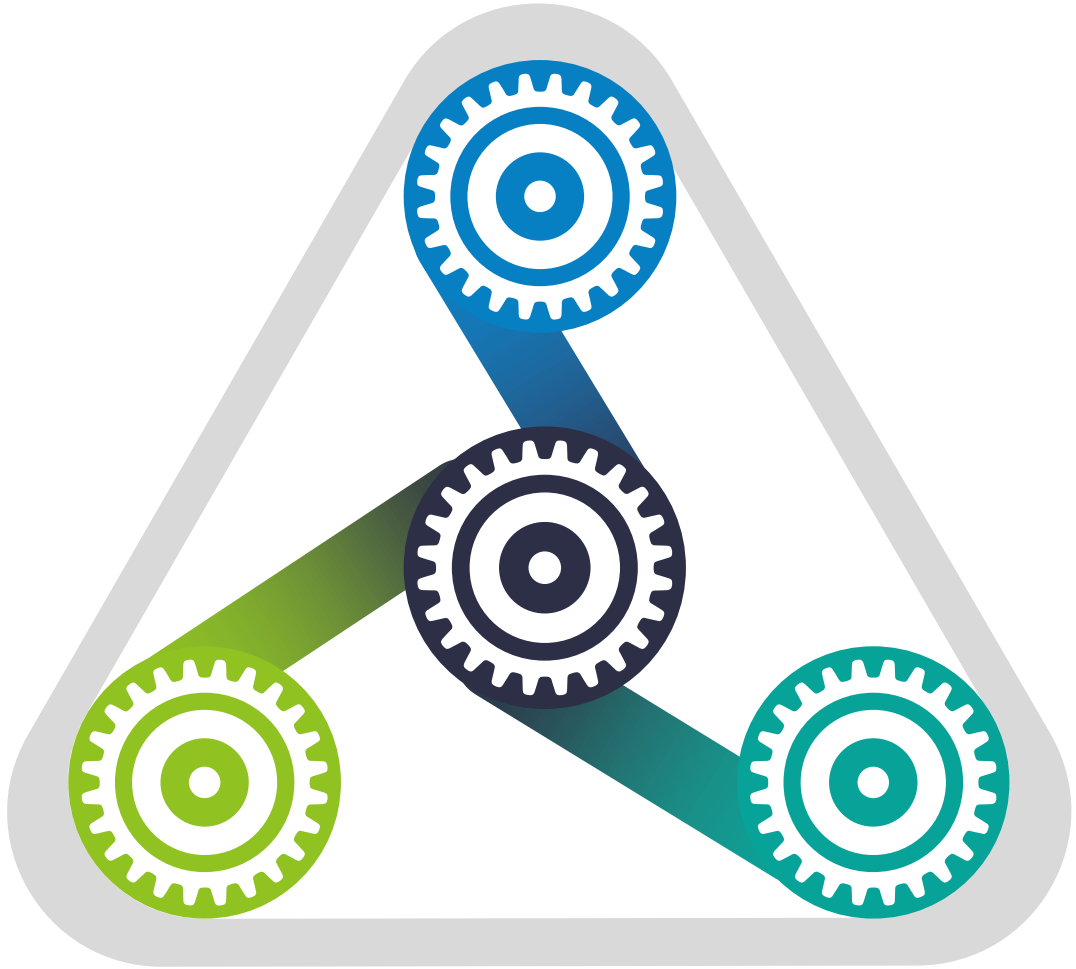
Il malware è preinstallato sullo spazio di memoria del dispositivo, tra cui fotocamere, unità USB, registratori, telefoni e altro.



Settori Target

- Governo e Difesa
- Energia and Utilities
- Banche e Finanza
- Sanità
- Telecomunicazioni
- Piccole e Media Imprese (PMI)
- ..ETC

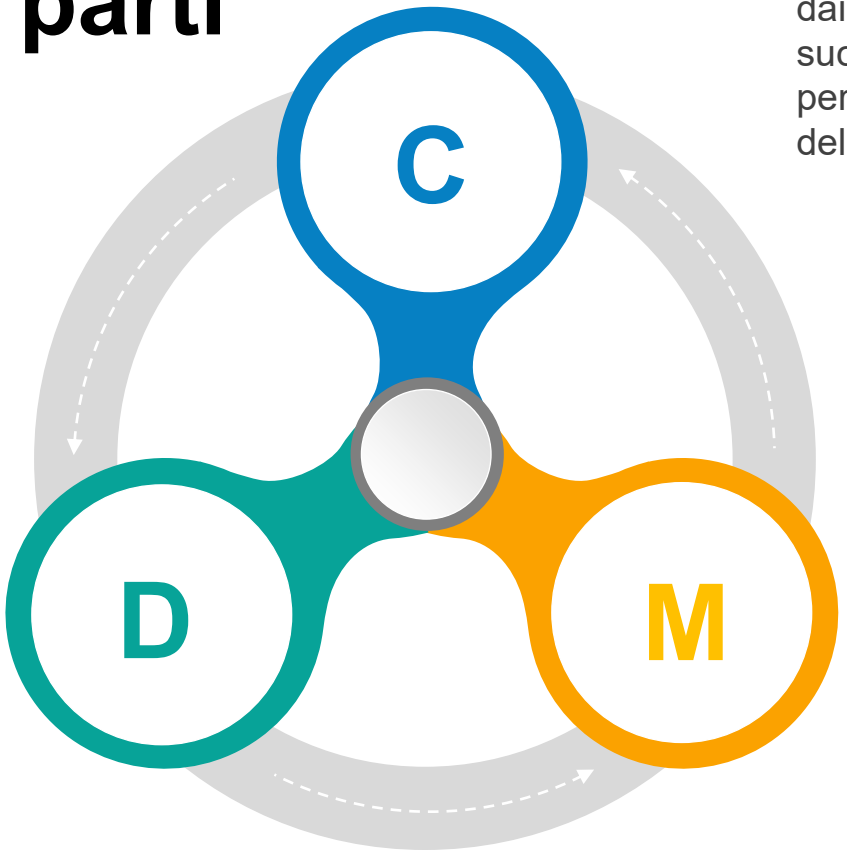
Perchè la Supply Chain Risk Management è importante?



- La dipendenza dai fornitori è in crescita
- Implicazioni per la sicurezza informatica
- Conseguenze finanziarie
- Conformità normativa

Rischi associati a fornitori di terze parti

I fornitori di terze parti svolgono un ruolo cruciale in molte aziende, fornendo beni, servizi e tecnologie che le organizzazioni potrebbero non essere in grado di sviluppare o gestire internamente.



Cyberattacks

I fornitori possono essere presi di mira dai criminali informatici e, se violati con successo, possono fungere da gateway per gli aggressori per infiltrarsi nella rete dell'organizzazione.

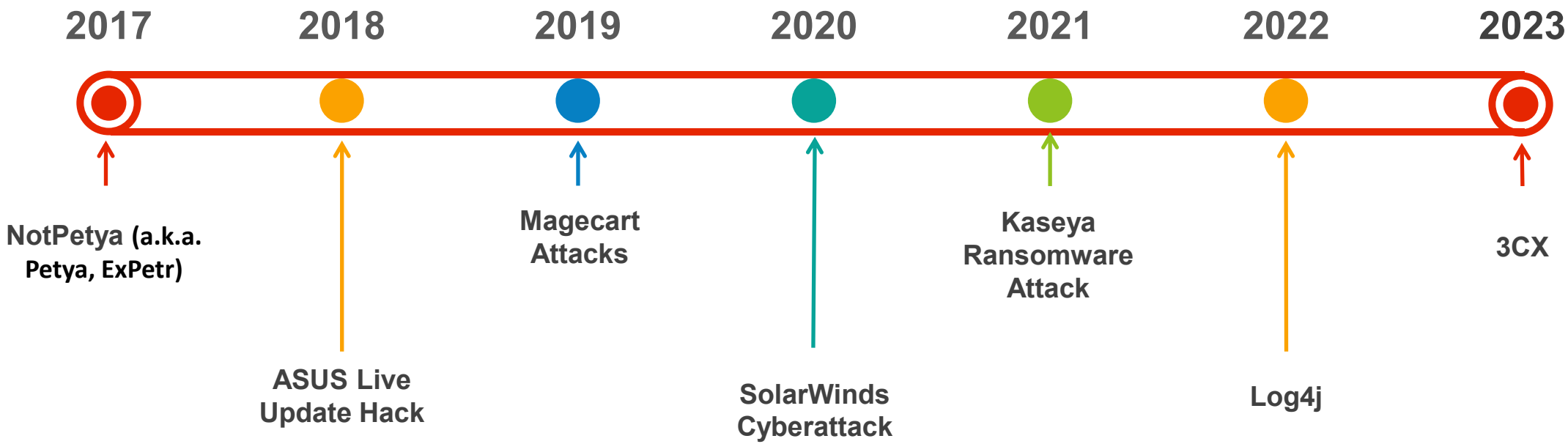
Data Breaches

I fornitori hanno spesso accesso ai dati sensibili di un'organizzazione. Se le misure di sicurezza di un fornitore sono inadeguate, possono portare a violazioni dei dati e all'esposizione di informazioni riservate

Malware and Ransomware

Il software malevolo introdotto attraverso i sistemi di un fornitore può diffondersi in tutta la rete dell'organizzazione, causando interruzioni e perdite finanziarie.

Principali Attacchi alla Supply Chain



Valutazione dei rischi per la sicurezza informatica

Identifica risorse e dati

Identifica le minacce

Assess Vulnerabilities

Calcolare la Probabilità di rischio

Determinare l'impatto

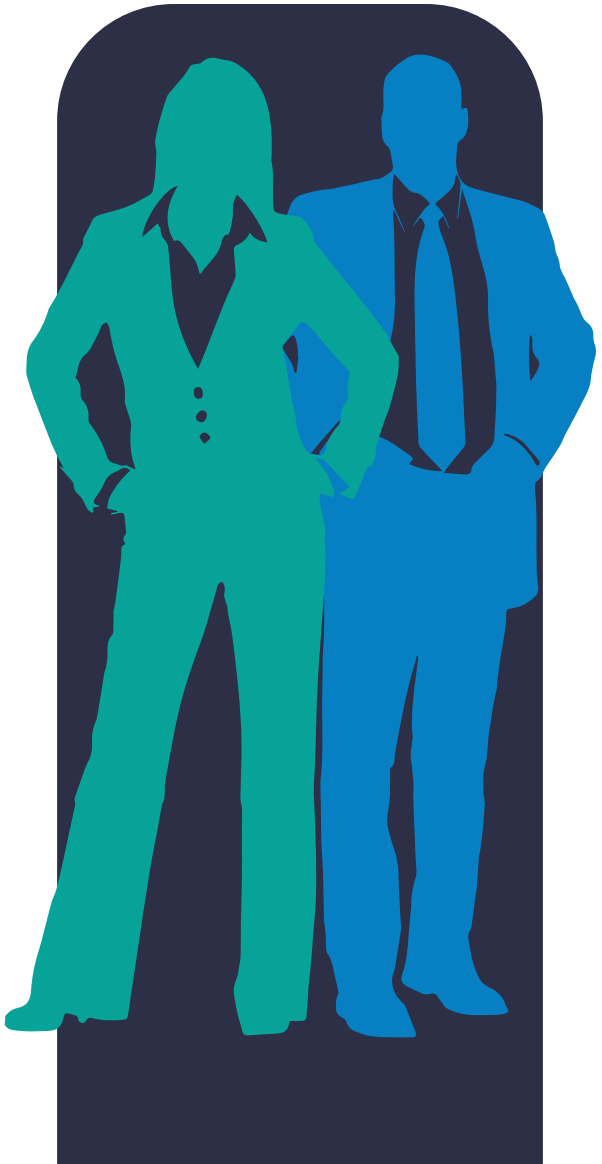
Valutazione del rischio

Valutazione del rischio del fornitore

Inventario dei fornitori
Iniziare creando un inventario completo di tutti i venditori, i fornitori e i fornitori di servizi di terze parti con cui la tua organizzazione interagisce.

Categorizzare i fornitori
Categorizzare i tuoi fornitori in base alla loro importanza e al livello di rischio che rappresentano per la tua organizzazione.

Definire i criteri di valutazione
Determinare i criteri e gli standard in base ai quali valuterai i tuoi fornitori.



Raccogliere informazioni sui fornitori
Richiedere informazioni e documentazione pertinenti ai fornitori.

Intervista i fornitori
Condurre interviste o discussioni con i rappresentanti dei fornitori per ottenere una comprensione più approfondita dei processi.

Valutare il punteggio del rischio
Valutare le risposte del fornitore e le informazioni raccolte in base ai tuoi criteri di valutazione.

I Framework del Supply Chain Risk

ISO 28000

ISO 28000 is an international standard that provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a supply chain security management system

NIST Cybersecurity Framework

this framework provides guidelines for managing and reducing cybersecurity risk, which includes supply chain risks.

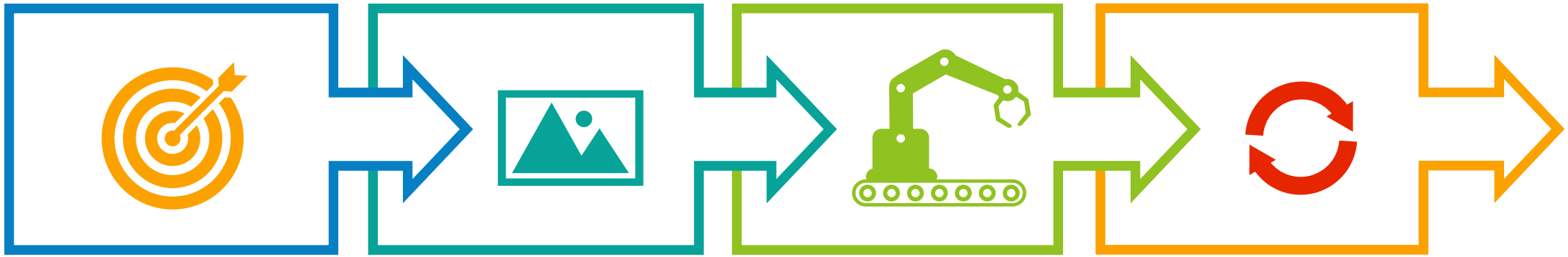
CIS Controls for Supply Chain Security

The Center for Internet Security (CIS) provides a set of cybersecurity controls specifically tailored for supply chain security

BSI Supply Chain Risk Management Standard

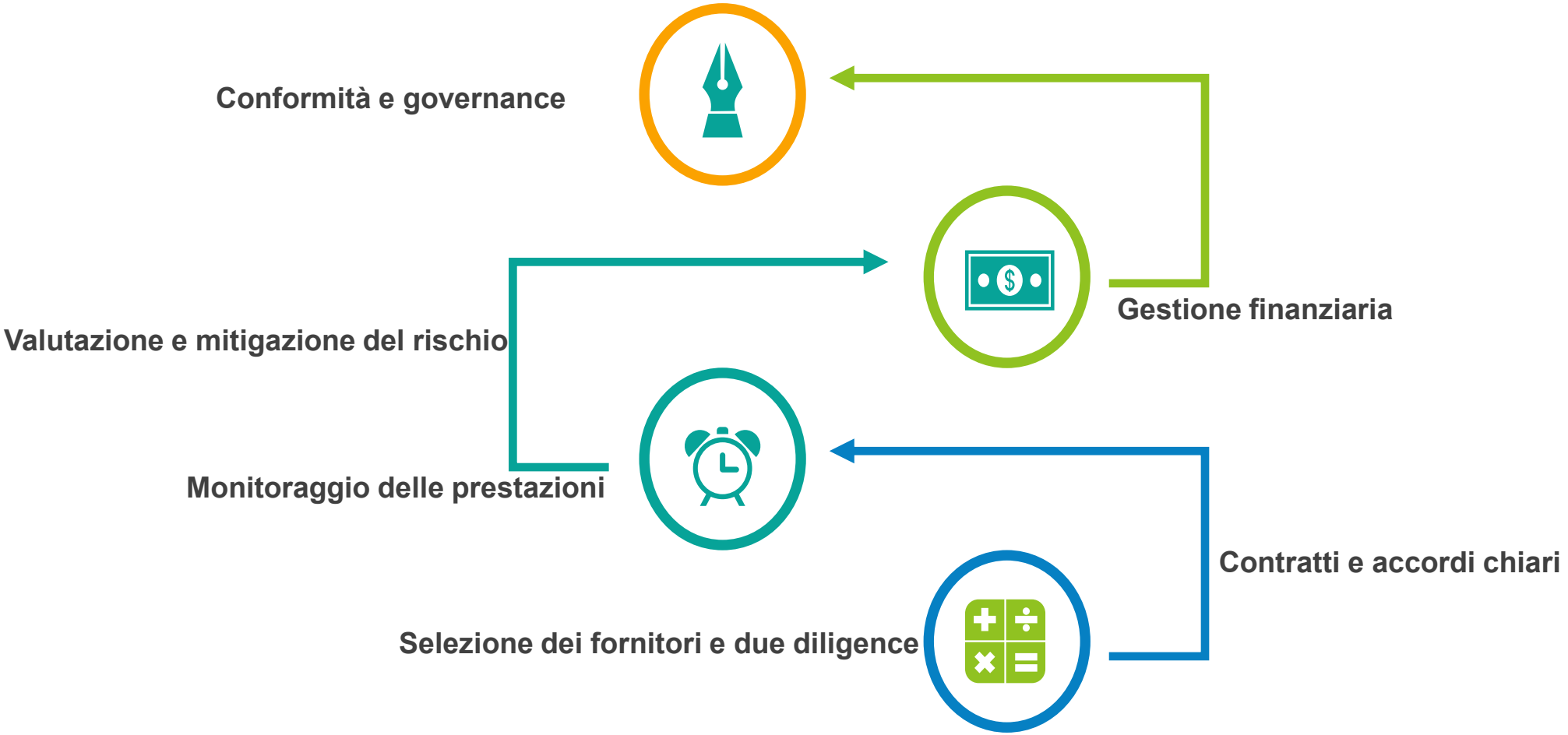
The British Standards Institution (BSI) has developed a supply chain risk management standard (BS 10500) that outlines best practices for identifying, assessing, and managing risks in the supply chain.

Valutazione del rischio del fornitore



- Identificare e comprendere i rischi
- Sviluppare una strategia di gestione del rischio
- Stabilire una regola chiara
- Monitoraggio continuo
- Piano di gestione delle crisi
- Formazione e sensibilizzazione dei dipendenti
- Backup e ripristino dei dati
- Conformità e normative

Gestione delle relazioni con i fornitori



Implementazione di strategie di approvvigionamento efficaci

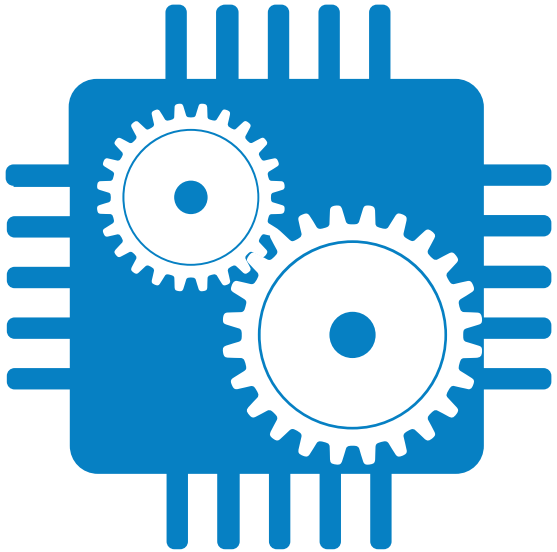
Stabilire obiettivi e traguardi chiari

Creare un team di approvvigionamento

Selezionare e valutare i fornitori

Controllo dei costi e gestione dei rischi

Gestione dei contratti



Grazie