CIPA | Convenzione Interbancaria per l'Automazione

15° Workshop – 9 giugno 2026

RILEVAZIONE SULL'IT NEL SETTORE BANCARIO ITALIANO

Profili tecnologici e di sicurezza

La Cybersecurity nel settore bancario: rischi e nuove minacce

Paola Paparo
Segreteria Tecnica CIPA

Partecipanti all'indagine
23 rispondenti

Allianz Bank Banca Agricola Popolare di Sicilia BNL

Banca Generali Banca IFIS Banca Passadore

Banca Popolare Pugliese Banco BPM

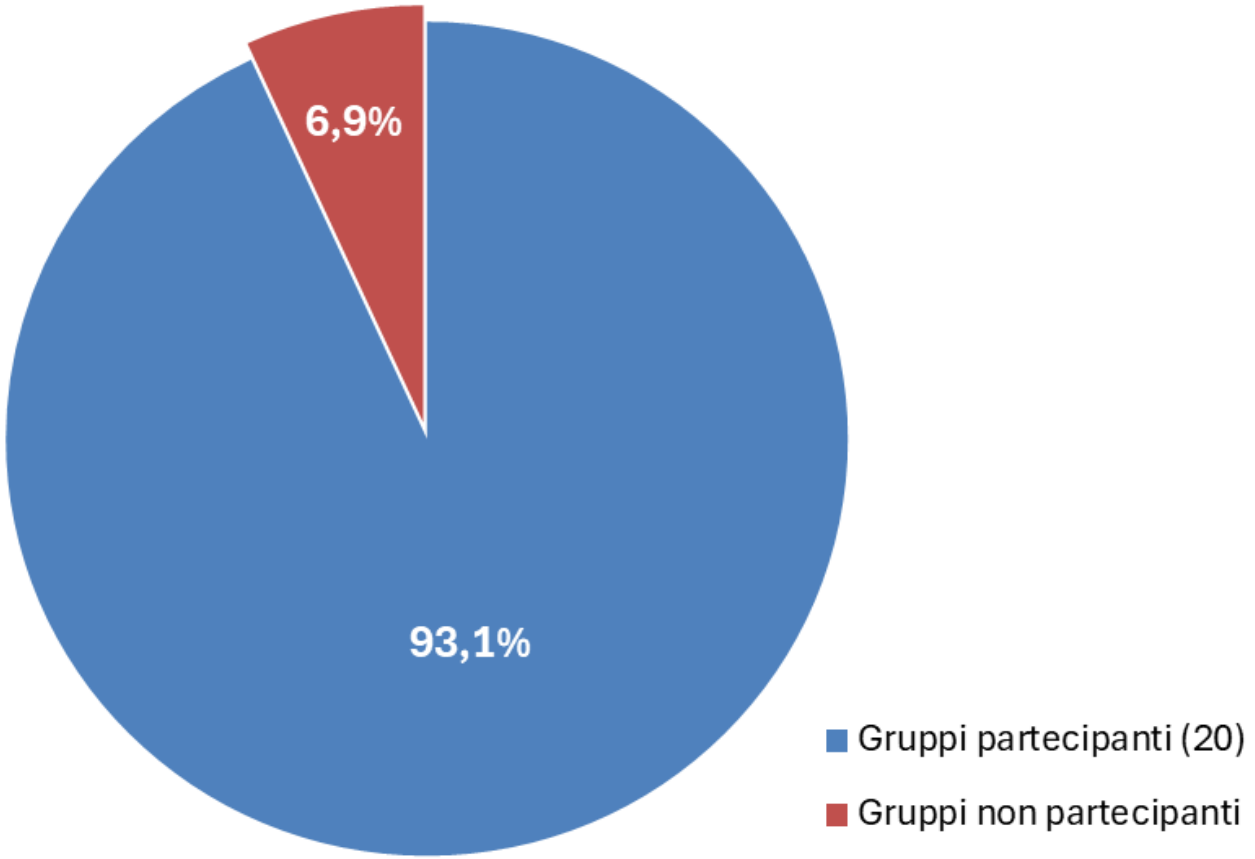
Banco Desio e Brianza BPER Banca Cassa Centrale Banca

Cassa Centrale Raiffeisen CR Asti CREDEM Crédit Agricole Italia

Deutsche Bank ICCREA Banca Intesa Sanpaolo

La Cassa di Ravenna Mediolanum MPS Sella Unicredit

Rappresentatività del campione – 20 Gruppi bancari
Totale attivo al 31/12/2025



PRESENTAZIONE

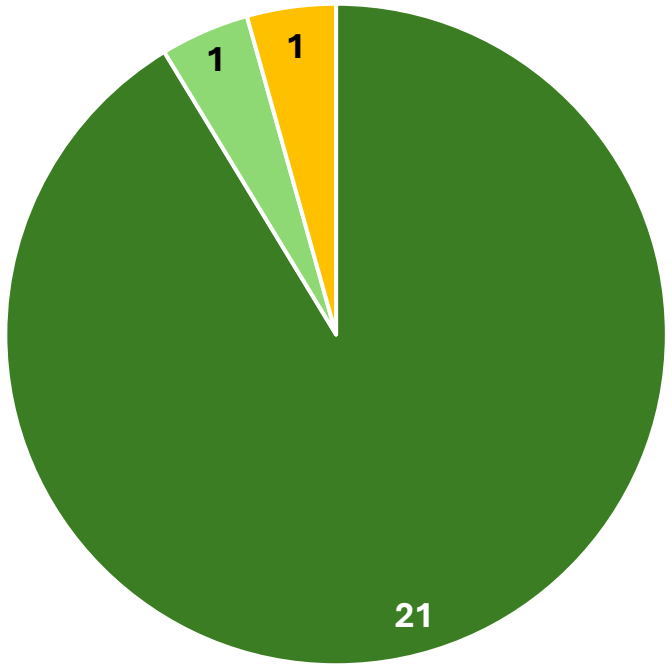
PRIMA PARTE

- Strategia, processi di sicurezza
- Aspetti economici e organizzativi
- Competenze

SECONDA PARTE

- Focus su alcuni processi di sicurezza
- Intelligenza Artificiale

STRATEGIA AZIENDALE PER LA SICUREZZA INFORMATICA



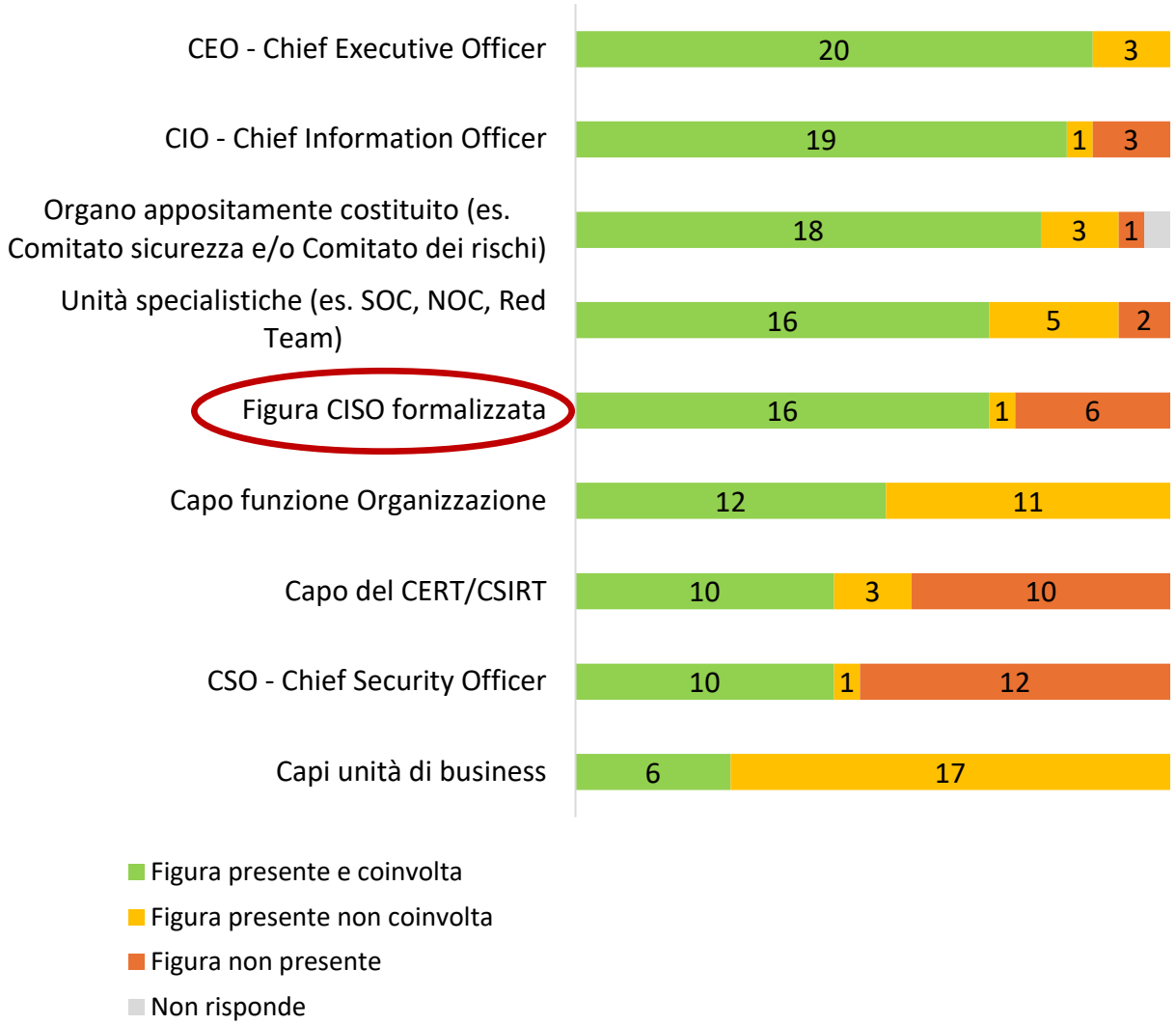
- Esiste e l'aggiornamento è previsto almeno ogni tre anni
- Esiste e l'aggiornamento è previsto almeno ogni cinque anni
- Esiste e l'aggiornamento avviene principalmente in seguito a incidenti gravi e/o nuove minacce rilevanti

23 rispondenti

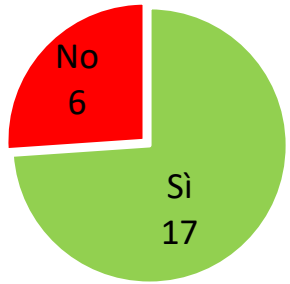
TEMATICHE DI SICUREZZA INDIRIZZATE NELLA STRATEGIA

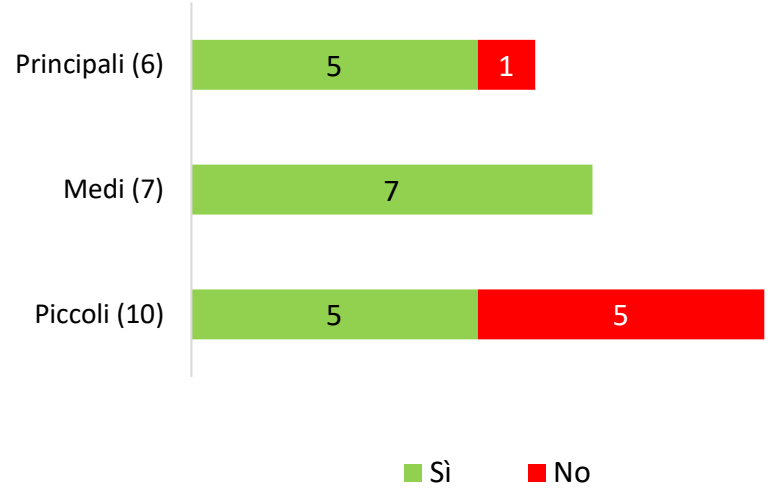
23 rispondenti

FIGURE COINVOLTE NELLA STRATEGIA DI SICUREZZA



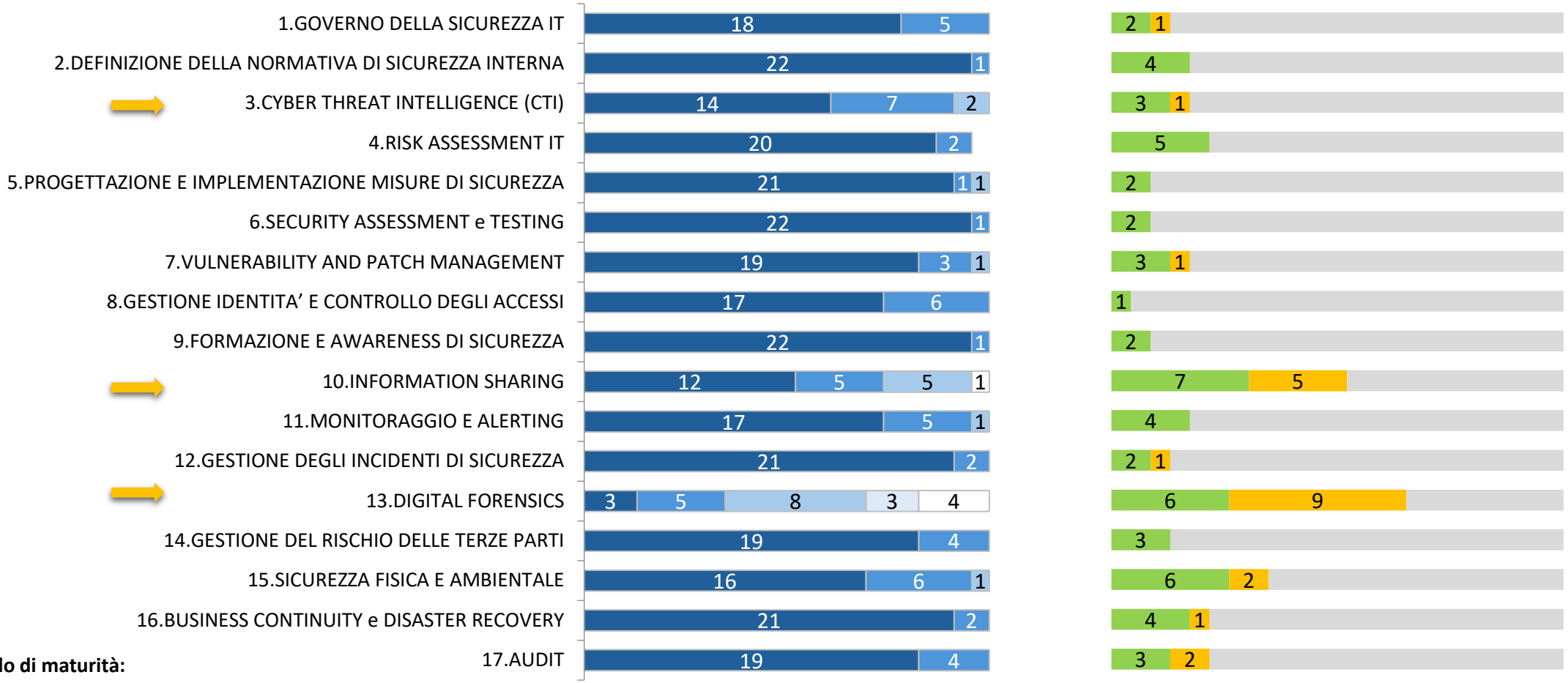
CISO – Chief Information Security Officer (figura formalizzata)





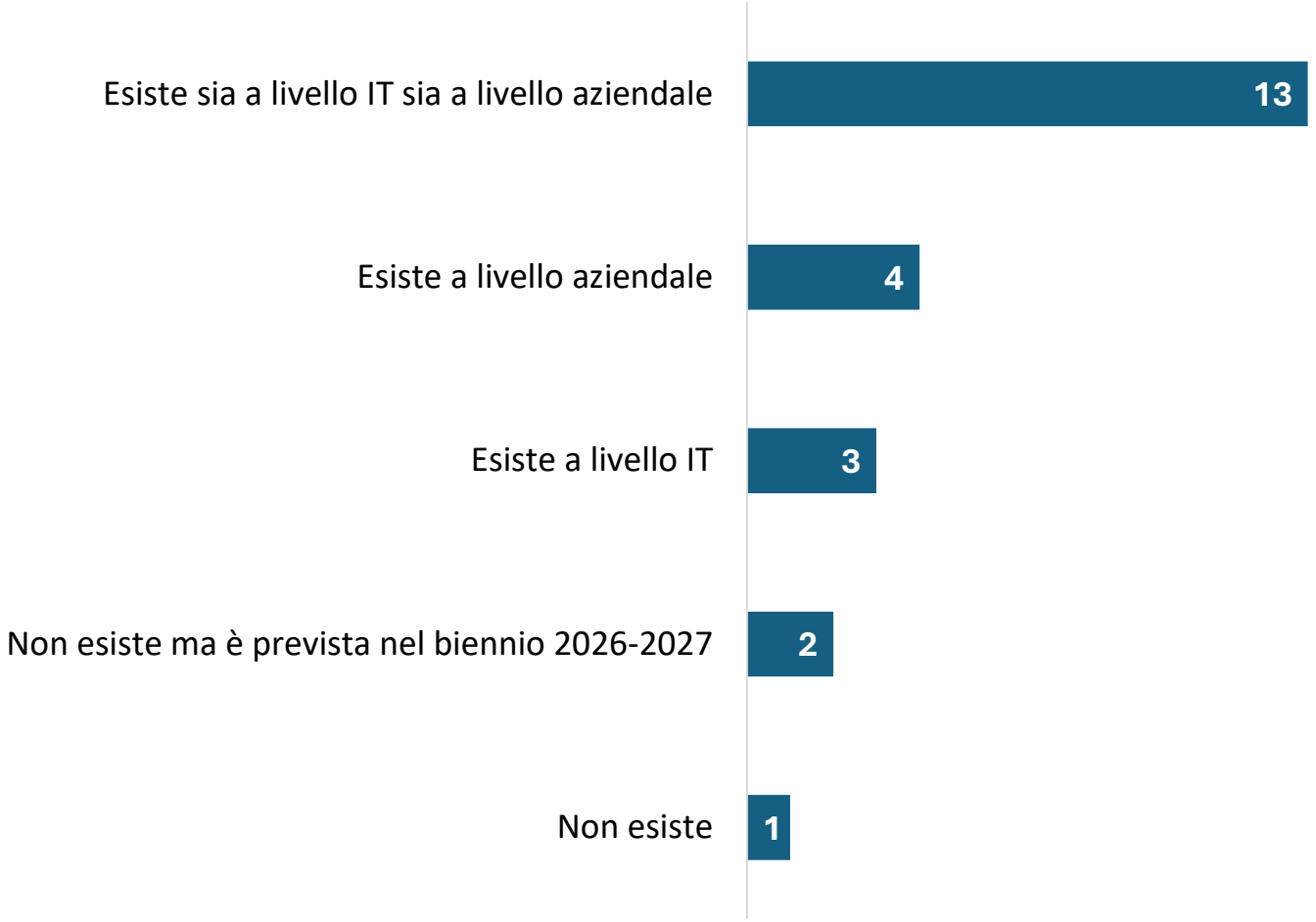
23 rispondenti

PROCESSI DI SICUREZZA - INIZIATIVE PROGETTUALI



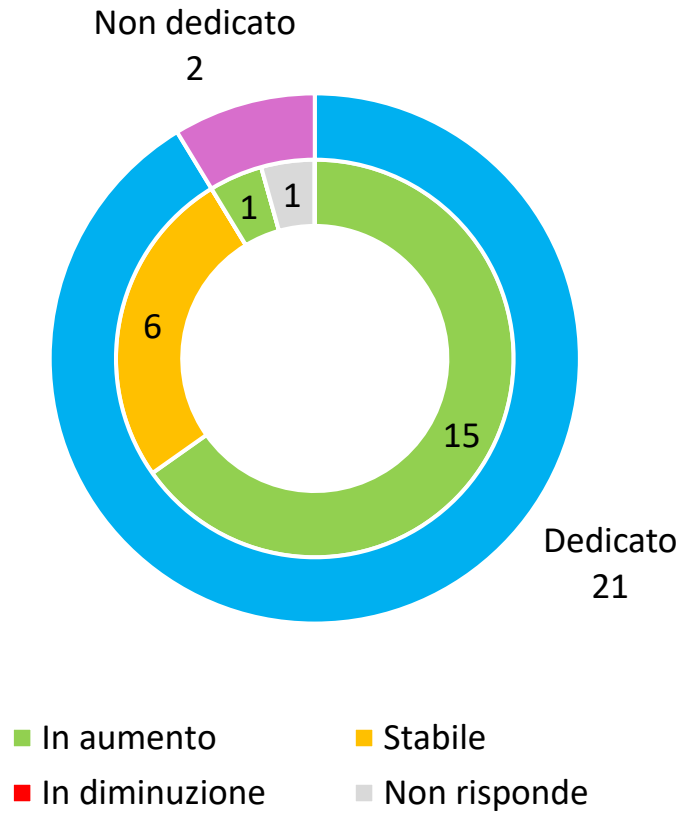
23 rispondenti

METODOLOGIA SPECIFICA PER I COSTI DI SICUREZZA

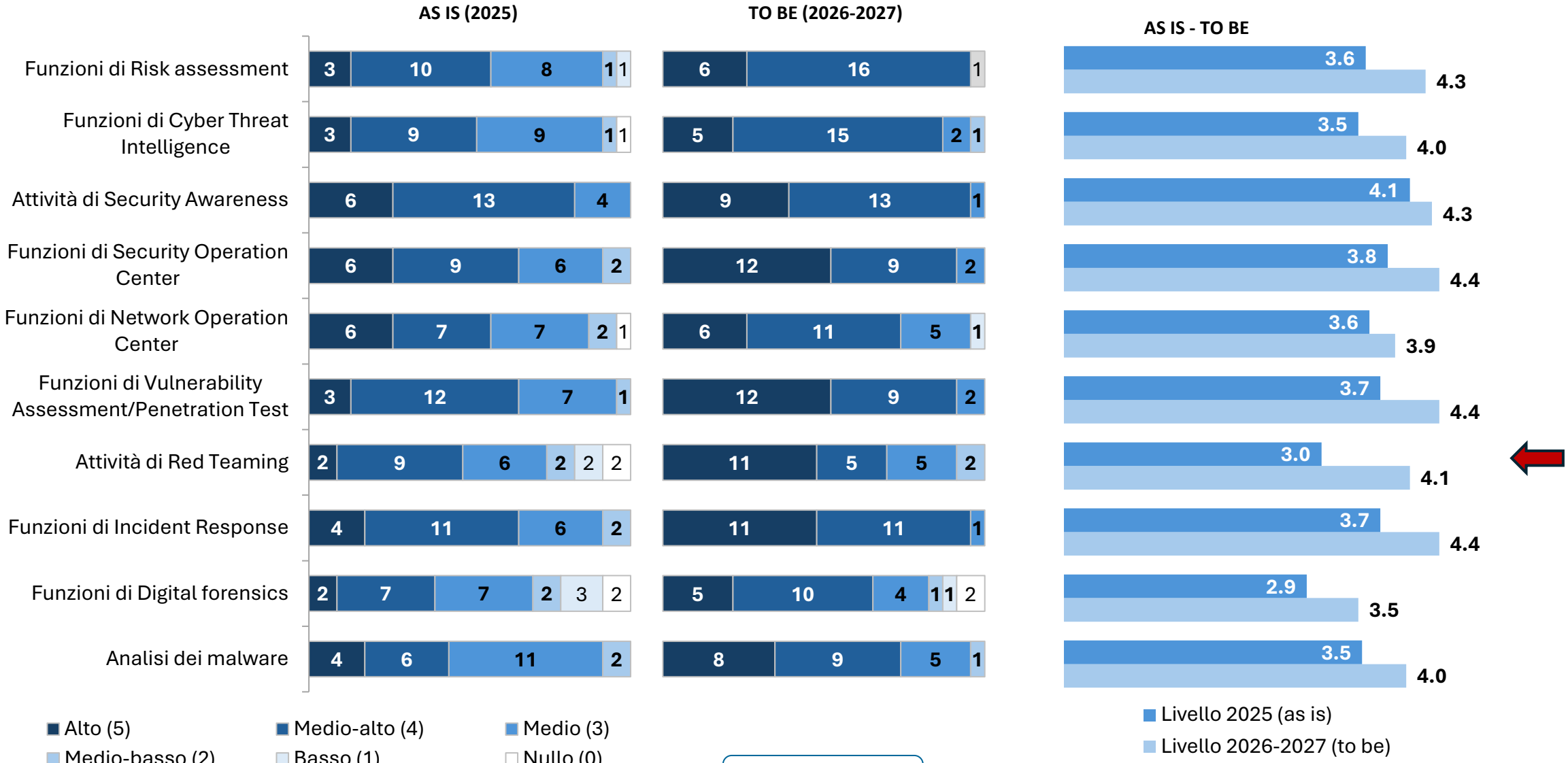


23 rispondenti

BUDGET IT 2026
(per le spese correnti)



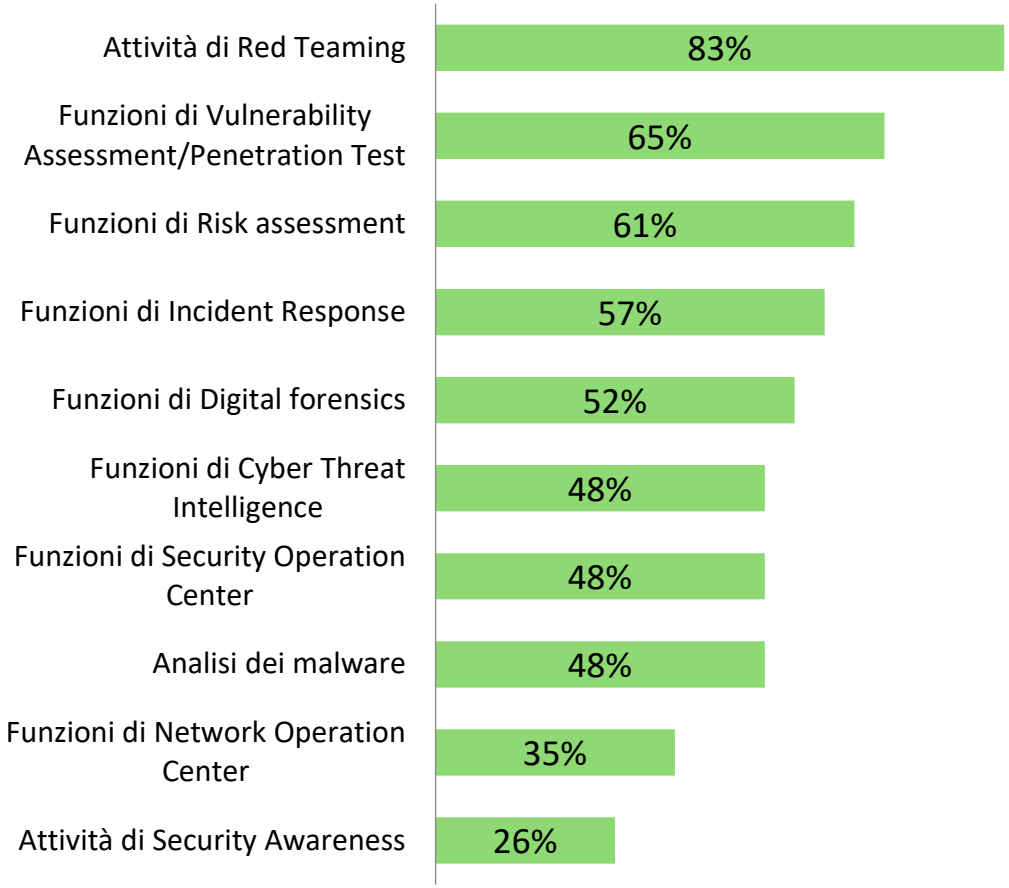
COMPETENZE (1)



23 rispondenti

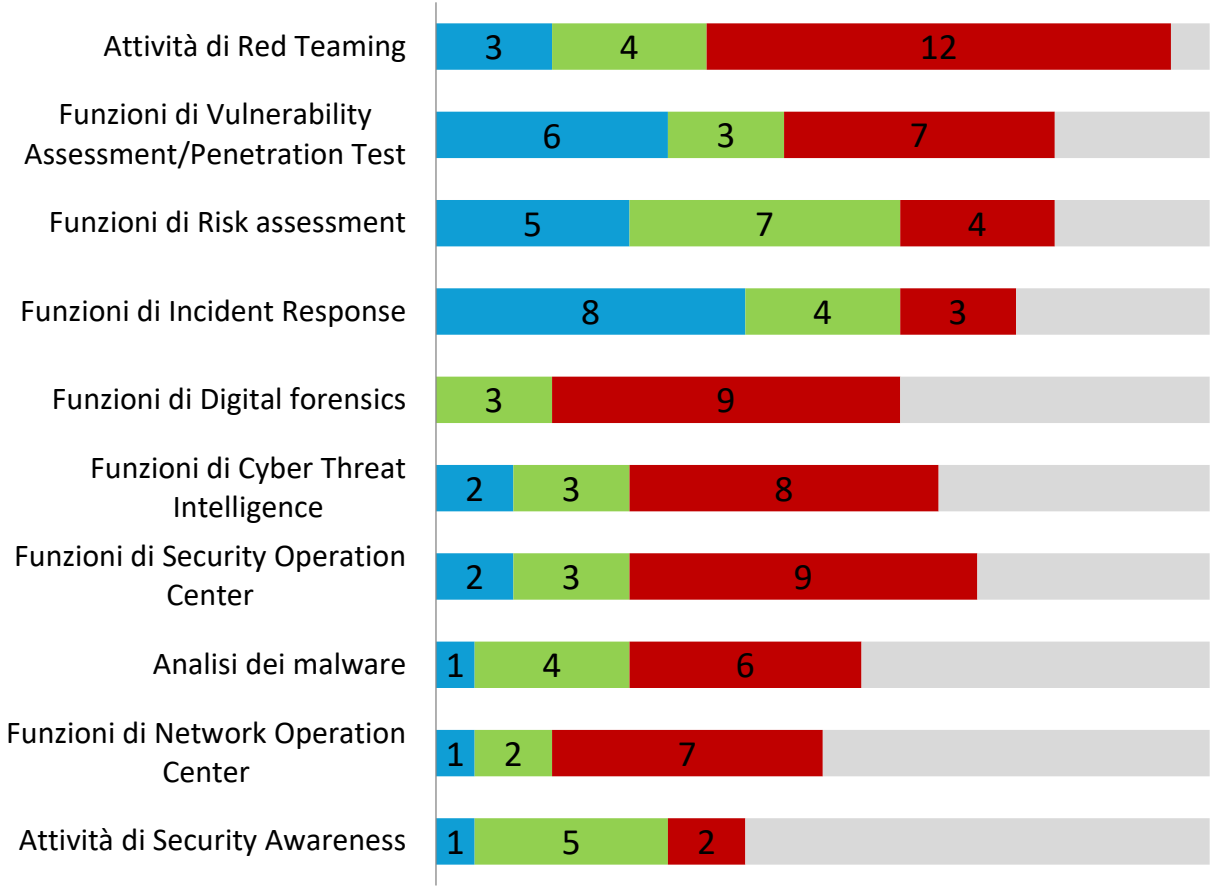
COMPETENZE (2)

GAP



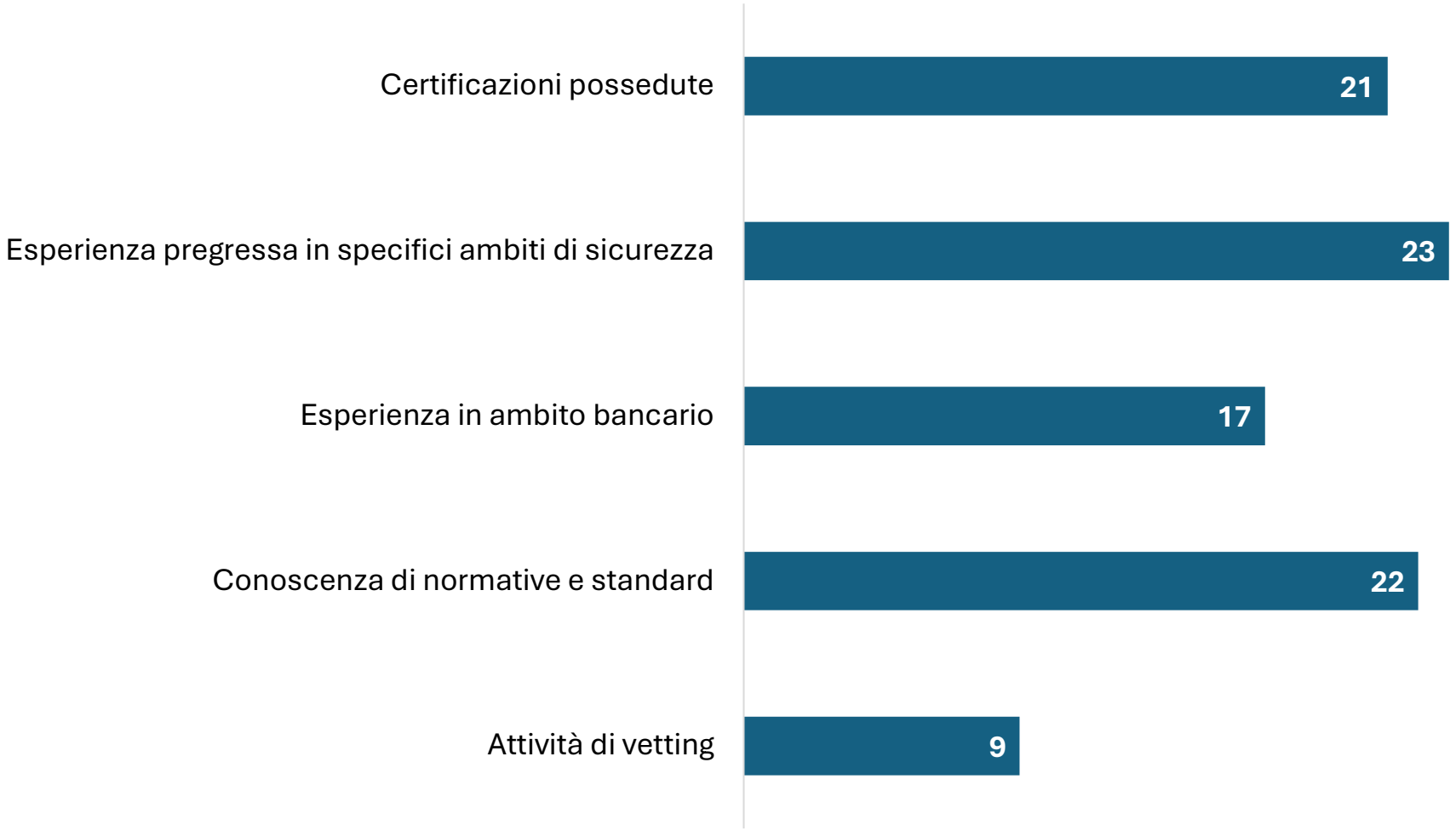
23 rispondenti

MODALITA' DI REPERIMENTO



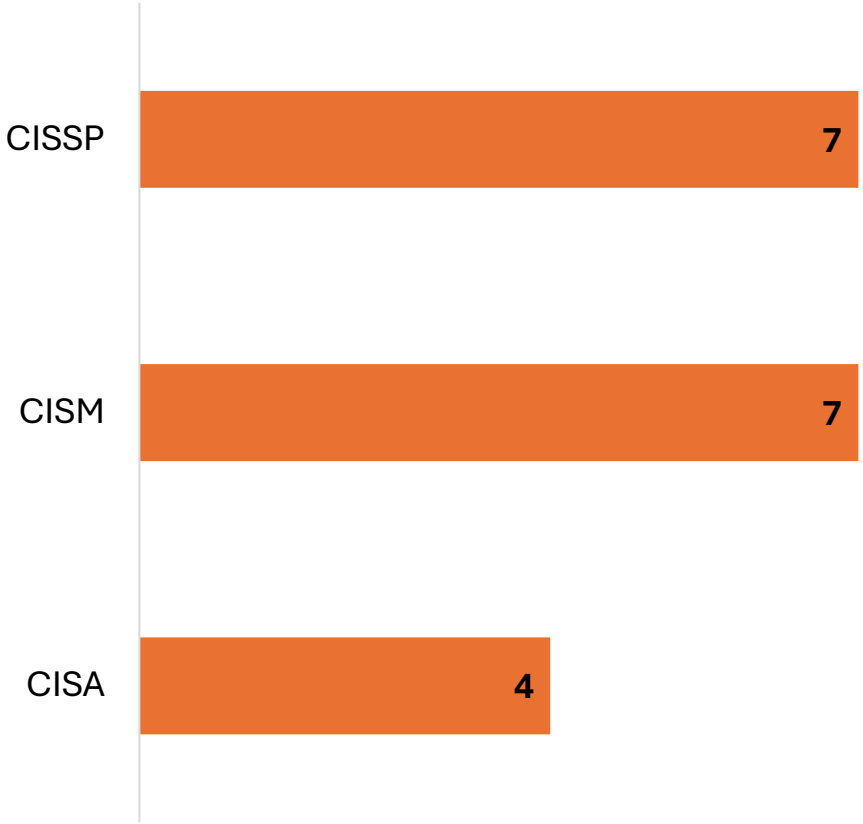
20 rispondenti

REQUISITI PER L'ASSUNZIONE

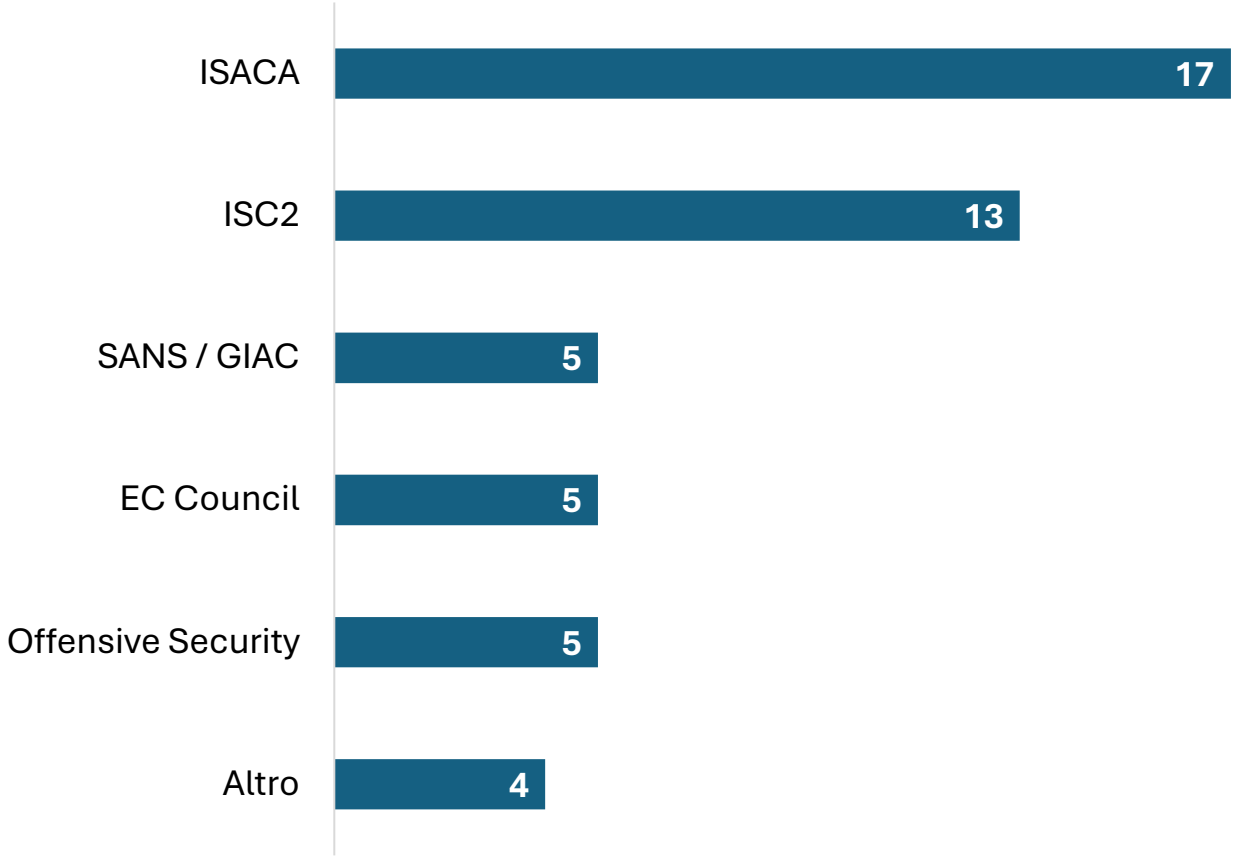


23 rispondenti

CERTIFICAZIONI - ISTITUTI DI FORMAZIONE

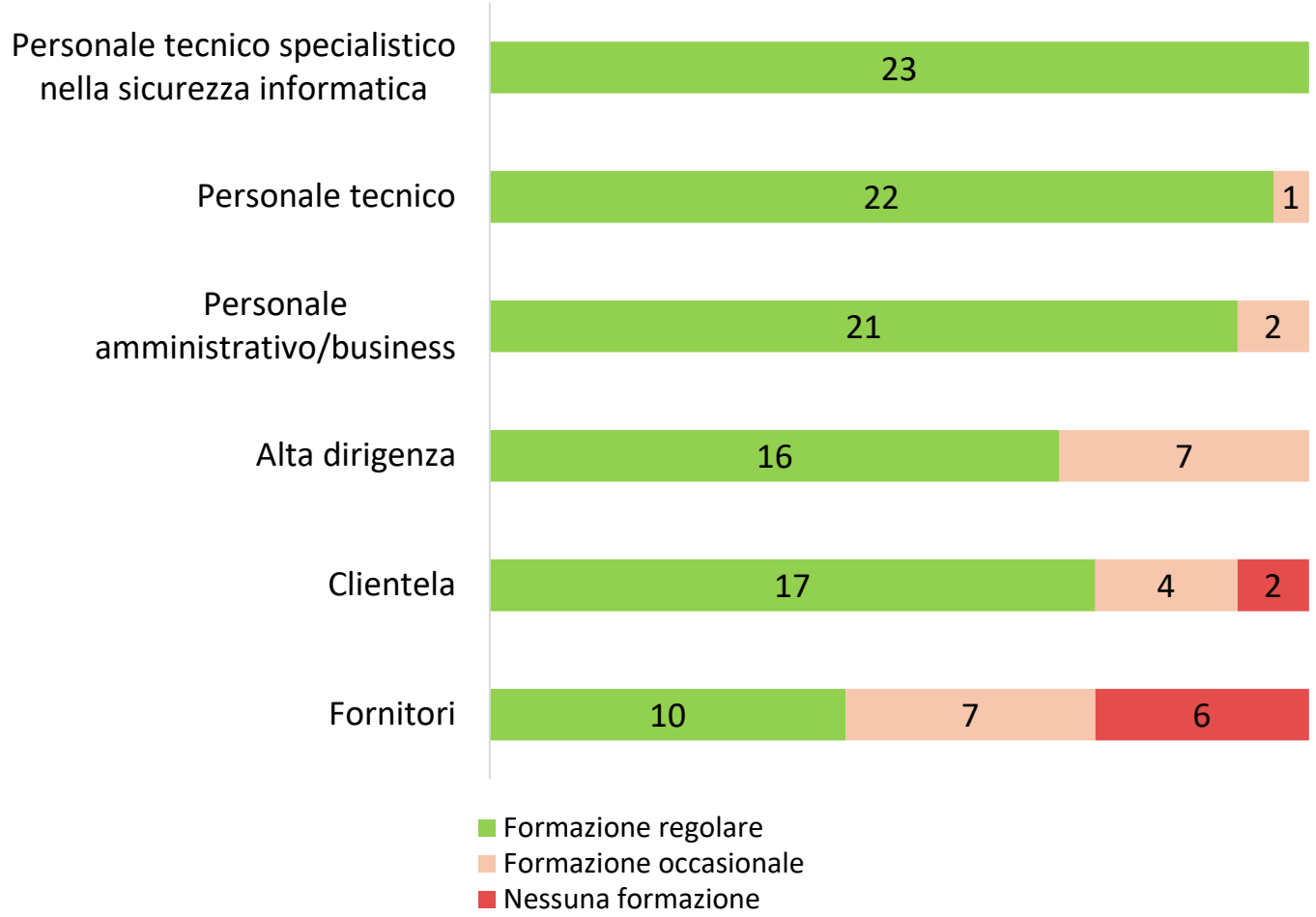


10 rispondenti



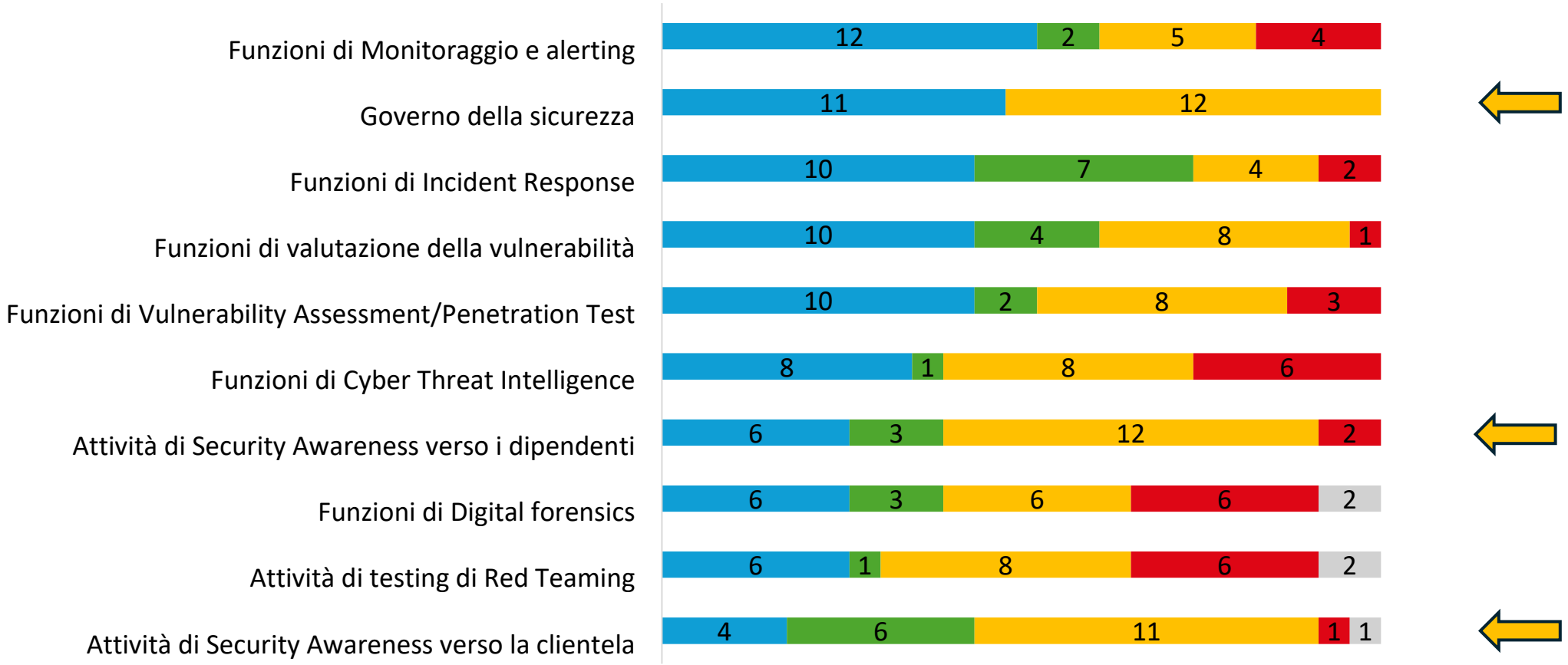
21 rispondenti

FORMAZIONE DEL PERSONALE



23 rispondenti

COLLOCAZIONE ORGANIZZATIVA DELLE FUNZIONI DI SICUREZZA



23 rispondenti

PRESENTAZIONE

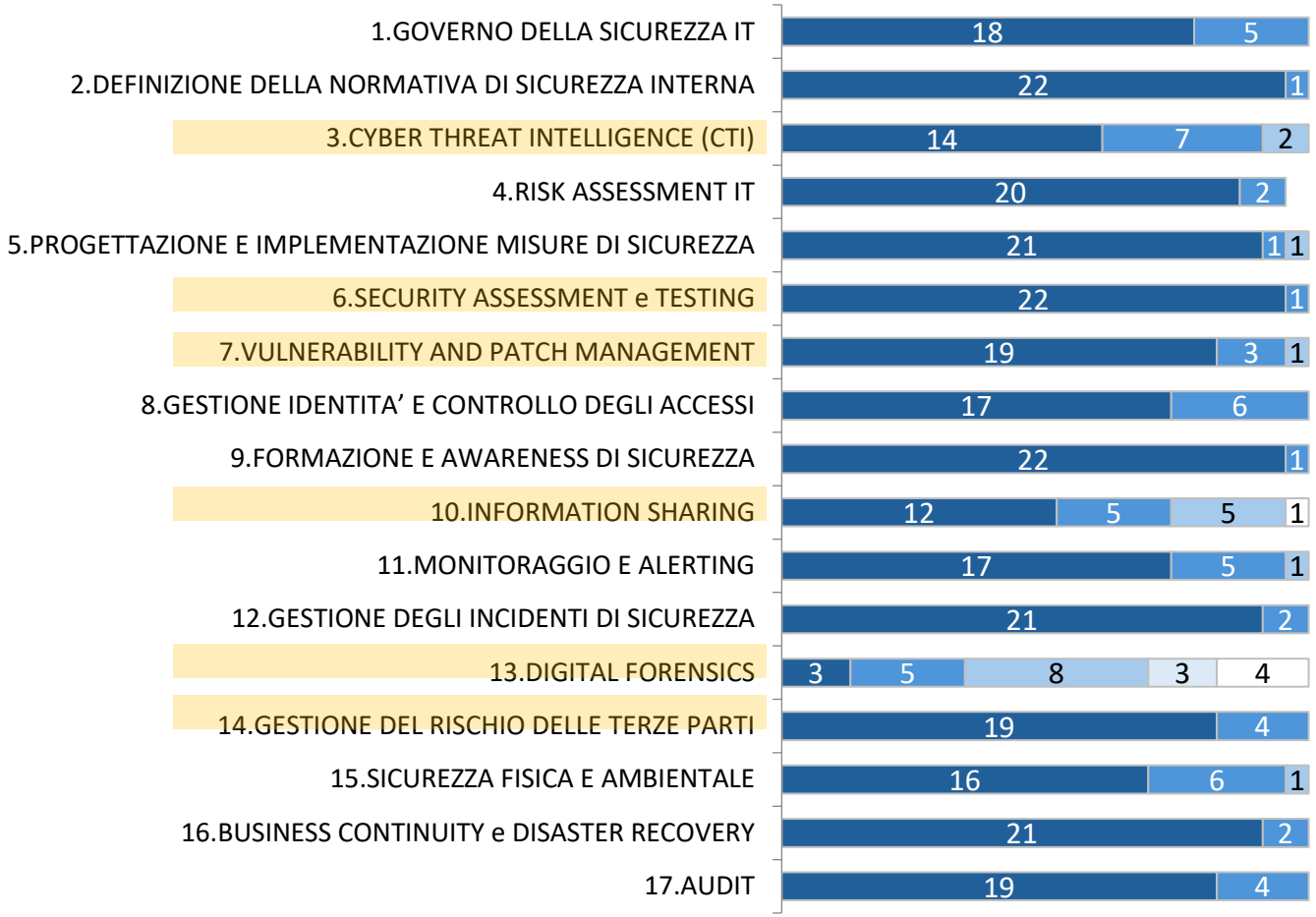
PRIMA PARTE

- Strategia, tematiche indirizzate, processi di sicurezza
- Aspetti economici e organizzativi
- Competenze

SECONDA PARTE

- **Focus su alcuni processi di sicurezza**
- **Intelligenza Artificiale**

Focus su PROCESSI DI SICUREZZA



Livello di maturità:

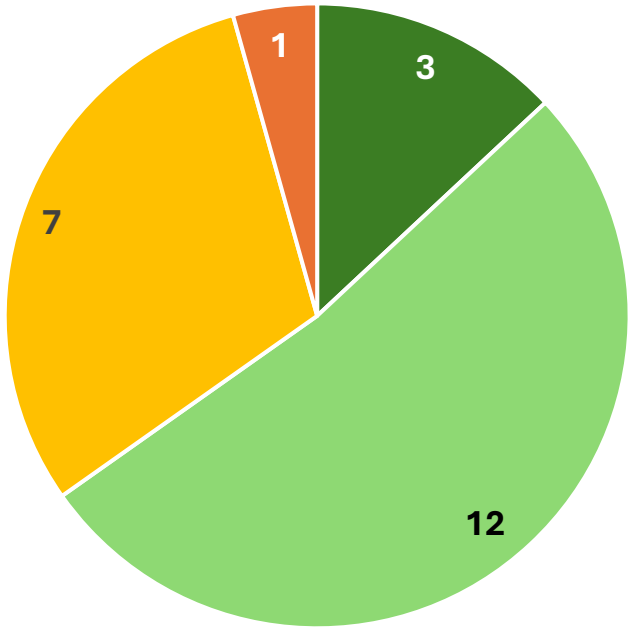
- 4 = Formalizzato e aggiornato sistematicamente
- 3 = Formalizzato ma non aggiornato sistematicamente
- 2 = Definito ma non formalizzato
- 1 = Presente ma non definito o formalizzato
- 0 = Non presente

23 rispondenti

Focus su CYBER THREAT INTELLIGENCE (1)

✅ **CYBER THREAT INTELLIGENCE**

Raccolta, analisi e interpretazione di informazioni relative alle minacce informatiche per il supporto alle decisioni strategiche, tattiche e operative.

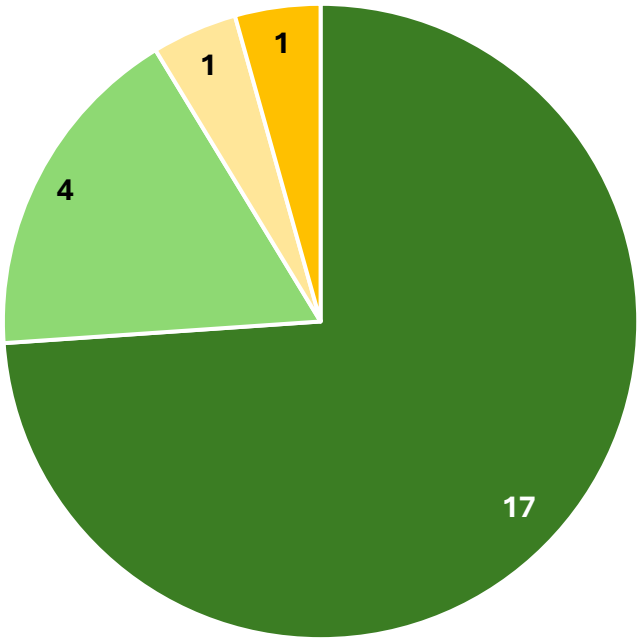


VALUTAZIONE STRATEGICA

- Il livello di minaccia cyber viene valutato e considerato nei piani di continuità operativa e di gestione della crisi
- Il livello di minaccia cyber viene valutato, qualificato e considerato nell'analisi dei rischi
- Il livello di minaccia cyber viene valutato solo nella produzione di report strategici periodici
- Il livello di minaccia cyber non viene valutato

23 rispondenti

Focus su CYBER THREAT INTELLIGENCE (2)



VALUTAZIONE OPERATIVA

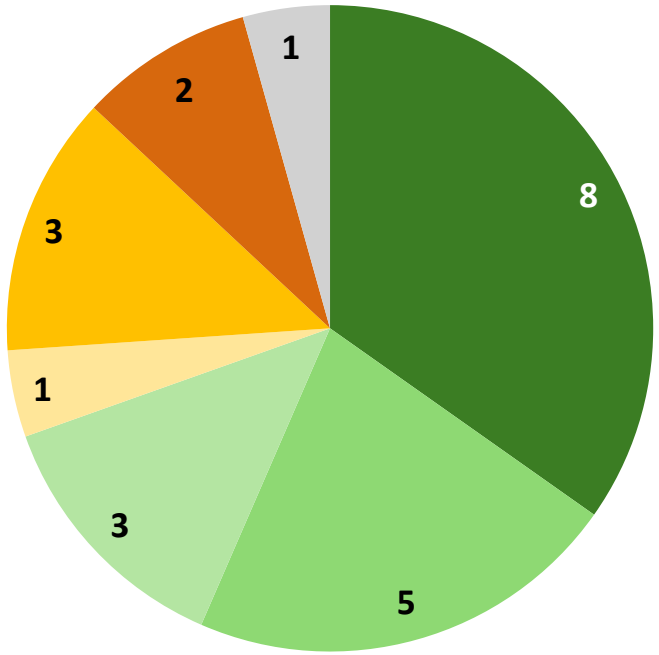
- Adattamento dinamico dei presidi di difesa (es. prioritizzazione delle vulnerabilità, azioni di mitigazione)
- Ricerca proattiva di minacce all'interno del perimetro, a partire da IOC e TTP
- Aggiornamento automatico dei sistemi di sicurezza in base agli IOC e/o Correlazione di tattiche, tecniche e procedure (TTP) con dati interni
- Raccolta, analisi e condivisione di indicatori di compromissione (IOC)

23 rispondenti

Focus su SECURITY ASSESSMENT E TESTING – Red Teaming

✅ **TEST DI RED TEAMING**

Attività di test avanzate mirate a verificare la postura di sicurezza e la capacità complessiva dell'organizzazione di essere resiliente.



TEST DI RED TEAMING

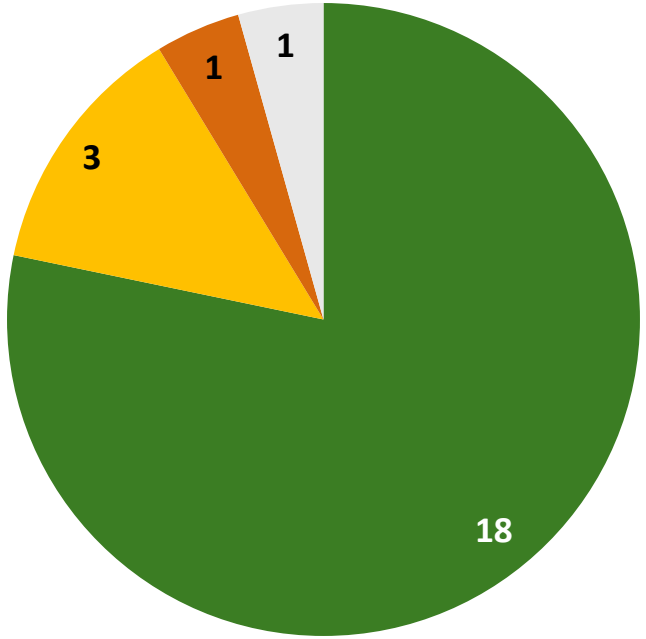
- Sono stati già eseguiti e sono regolarmente previsti almeno ogni anno
- Sono stati già eseguiti e sono regolarmente previsti almeno ogni tre anni
- Sono stati già eseguiti ma non sono previsti in modo sistematico
- Non sono stati ancora eseguiti ma sono regolarmente previsti almeno ogni anno
- Non sono stati ancora eseguiti ma sono regolarmente previsti almeno ogni tre anni
- Non sono stati né eseguiti e né sono previsti
- Altro

23 rispondenti

Focus su VULNERABILITY ASSESSMENT E PATCH MANAGEMENT

✅ **VULNERABILIY ASSESSMENT E PATCH MANAGEMENT**

Identificazione, analisi e valutazione delle vulnerabilità presenti in sistemi, reti e applicazioni e gestione degli aggiornamenti software e altre contromisure necessarie alla correzione.



PRIORITIZZAZIONE VULNERABILITA’

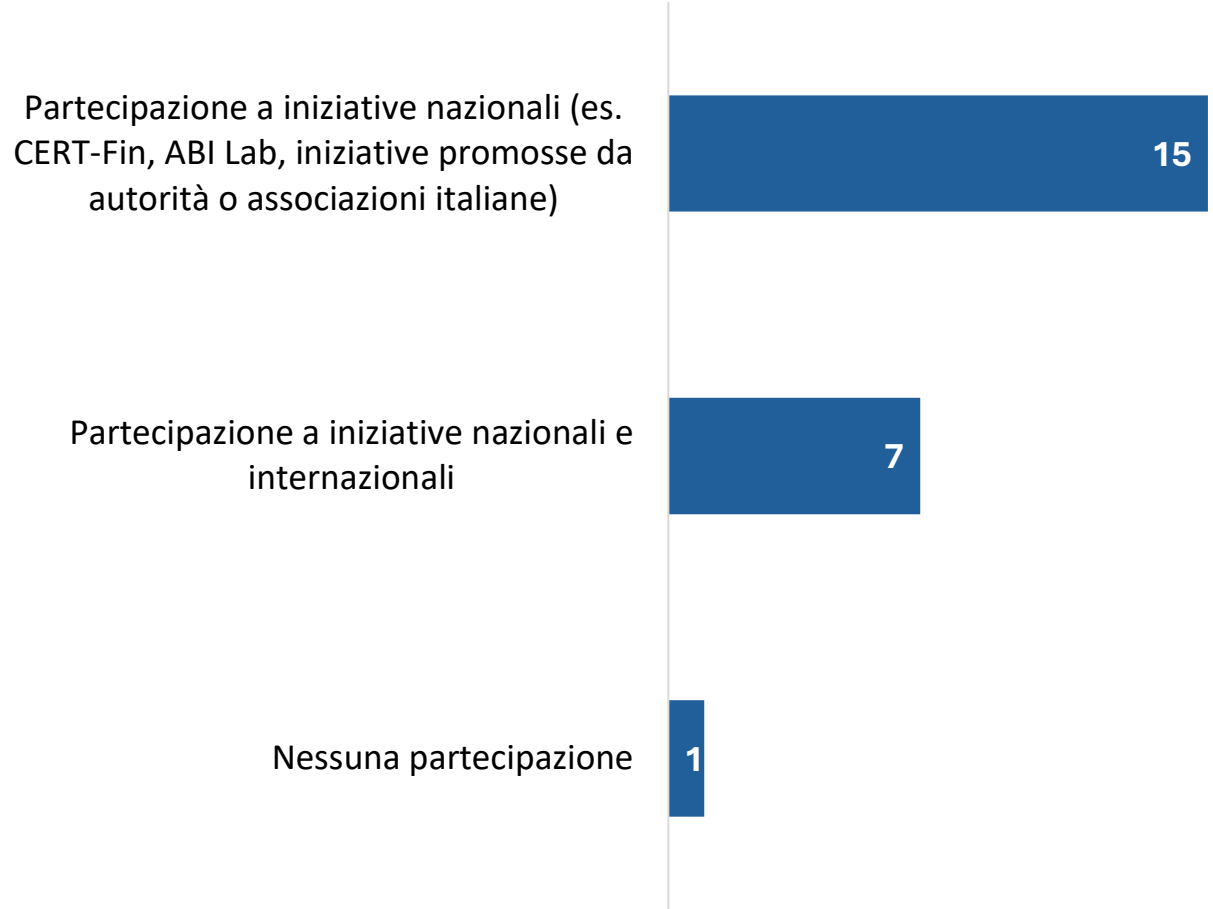
- Si tiene conto della criticità, della sfruttabilità e dell'esposizione della vulnerabilità
- Si tiene conto solo della criticità e della sfruttabilità della vulnerabilità
- Si tiene conto unicamente della criticità della vulnerabilità
- Altro

23 rispondenti

Focus su INFORMATION SHARING

✅ **INFORMATION SHARING**

Condivisione volontaria di dati, informazioni, attività di intelligence tra differenti organizzazioni nell'ambito di una «trusted community».

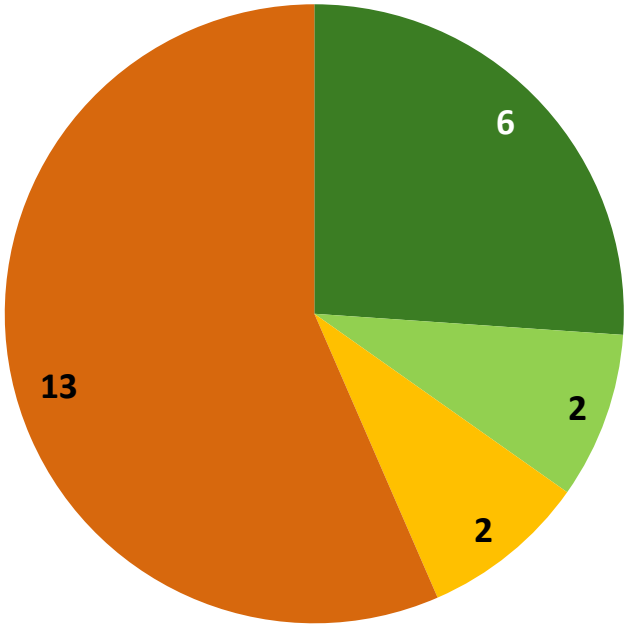


23 rispondenti

Focus su DIGITAL FORENSICS

✅ **DIGITAL FORENSICS**

Presentazione e conservazione delle evidenze digitali aventi valore probatorio dopo un incidente informatico.



POLICY DI FORENSIC READINESS

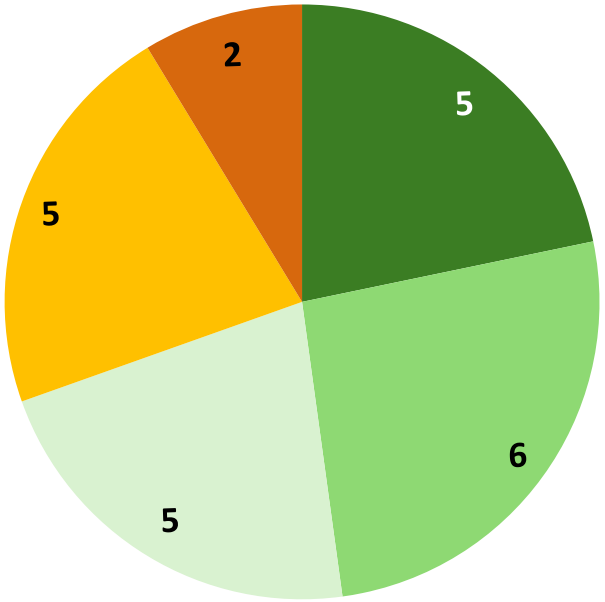
- La policy è stata definita ed è stato anche aggiornato il processo di gestione degli incidenti di sicurezza
- La policy è stata definita
- La policy non è stata definita, ma è in previsione
- La policy non è stata definita

23 rispondenti

Focus su GESTIONE DEL RISCHIO DI TERZE PARTI

✅ **GESTIONE DEL RISCHIO DI TERZE PARTI**

Identifica, governa e monitora i rischi derivanti dai fornitori.

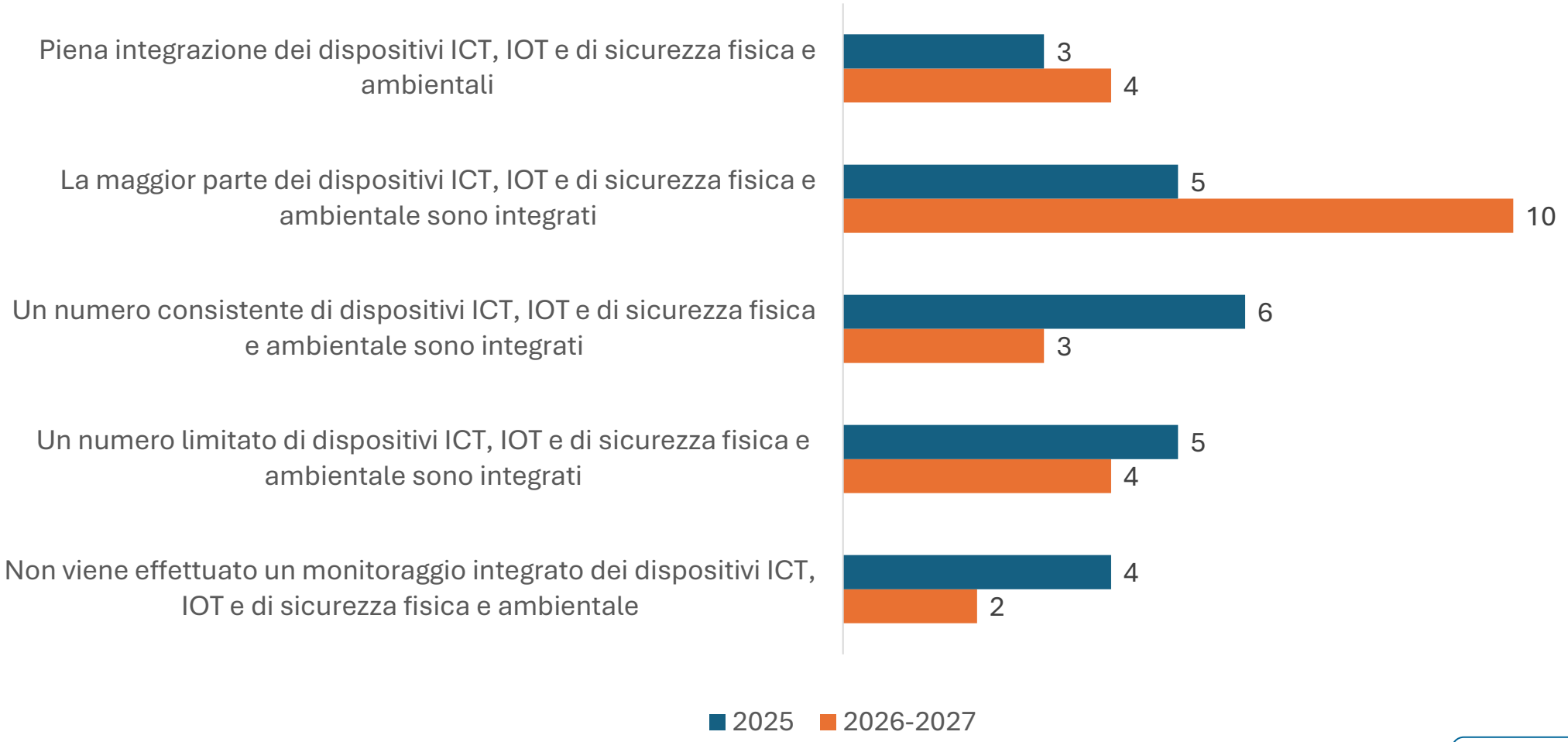


MONITORAGGIO AUTOMATIZZATO

- È automatizzato - applicato a tutti i fornitori
- È automatizzato - applicato solo ai fornitori critici
- È automatizzato - applicato alla maggior parte dei fornitori
- Non è automatizzato ma è in previsione
- Non è automatizzato

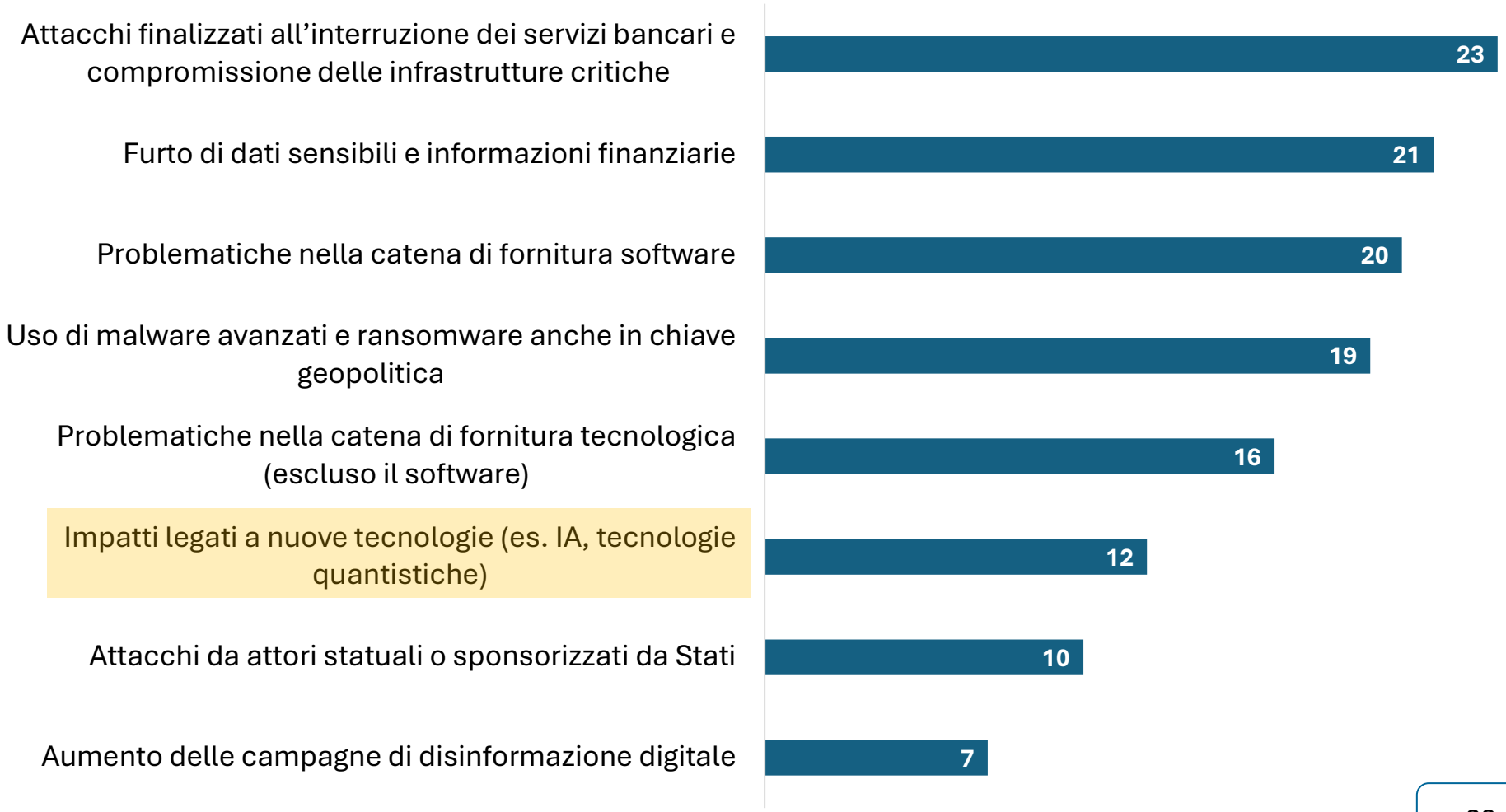
23 rispondenti

INTEGRAZIONE SICUREZZA FISICA E AMBIENTALE E LOGICA



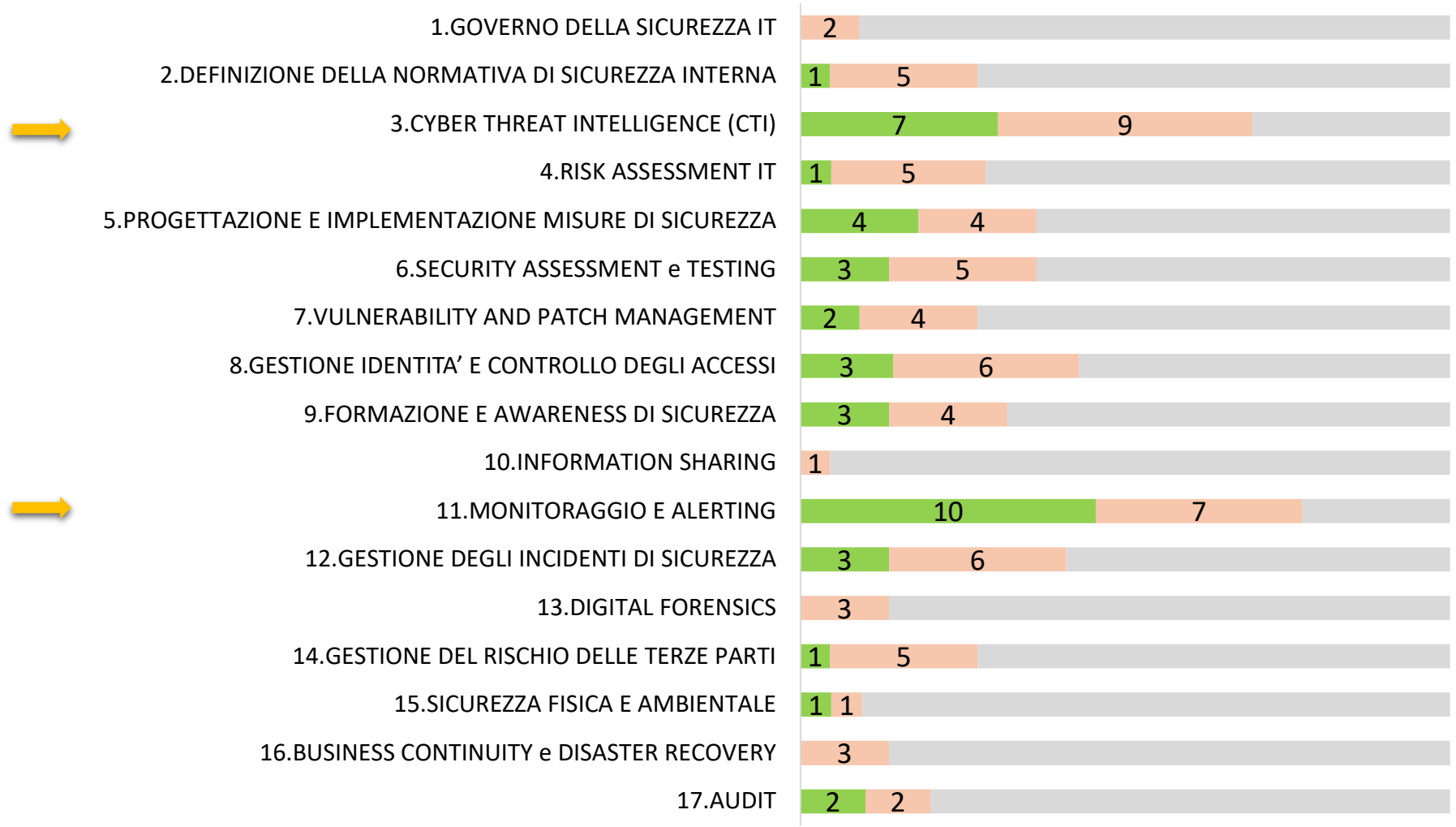
23 rispondenti

MINACCE CYBER CONSIDERATE NEL RISK ASSESSMENT



23 rispondenti

UTILIZZO DELL'INTELLIGENZA ARTIFICIALE NEI PROCESSI DI SICUREZZA



23 rispondenti

Grazie per l’attenzione

Segreteria Tecnica CIPA

La Cybersecurity nel settore bancario: rischi e nuove minacce