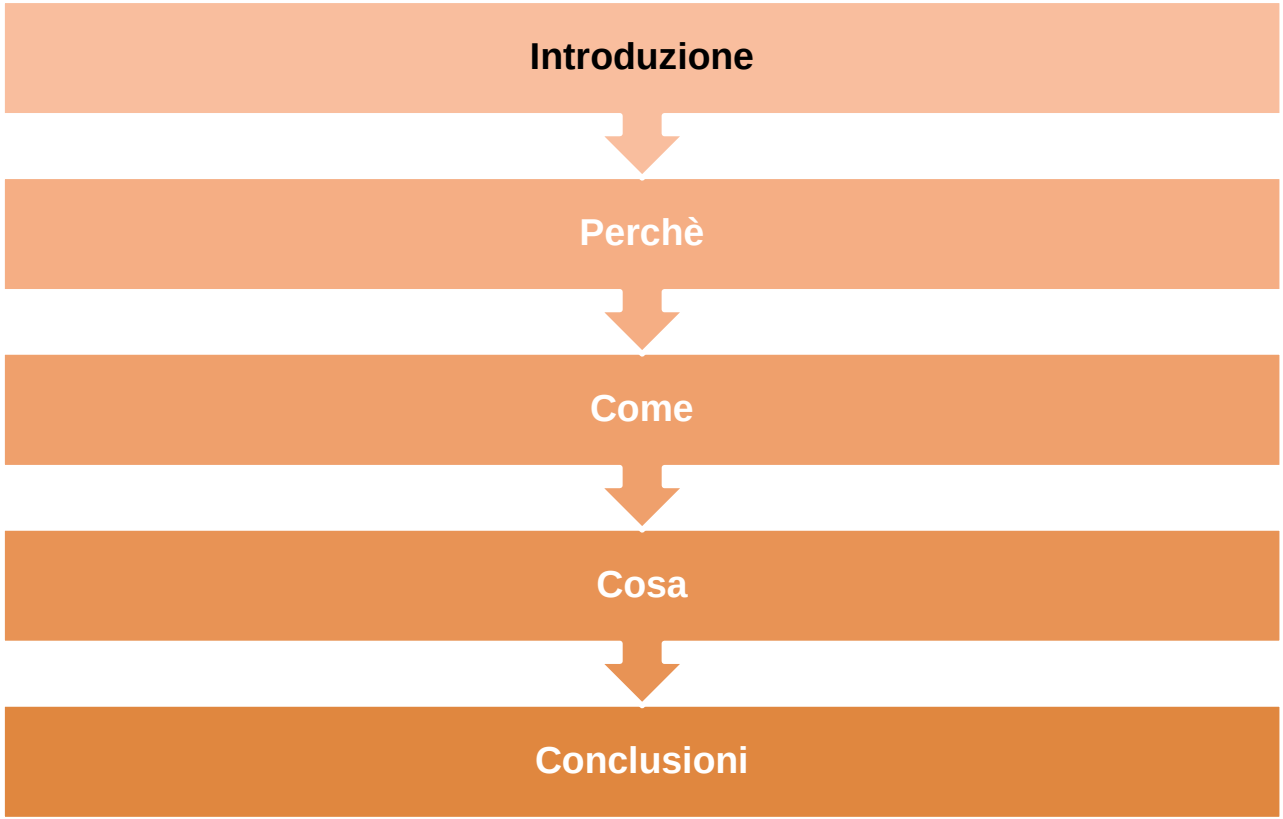
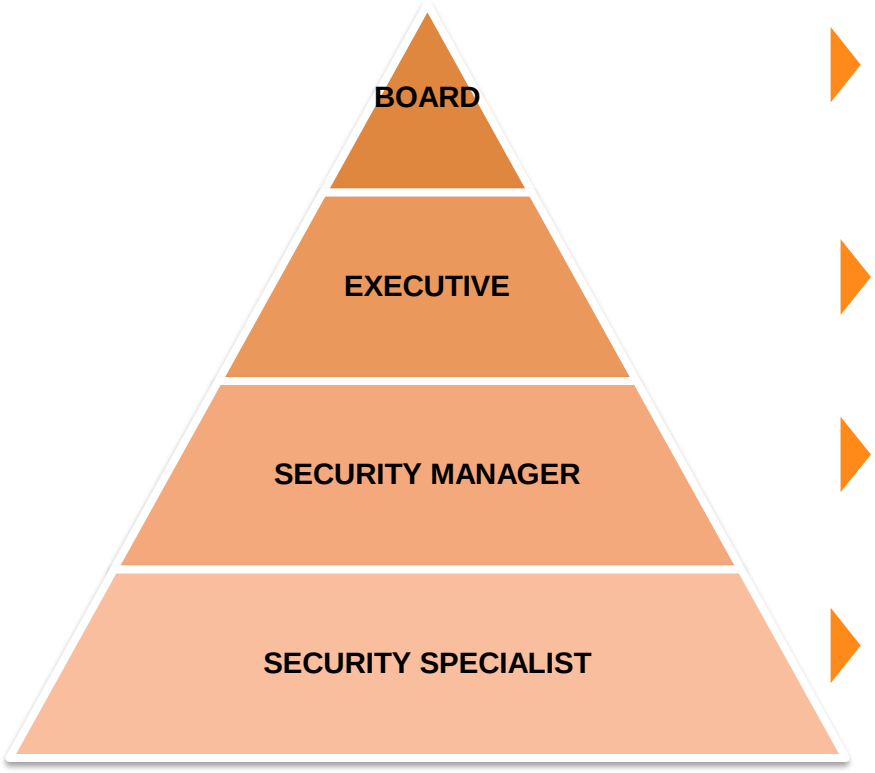
CyberSecurity Dashboard.
Dal mito alla realtà

Agenda



La trasparenza sulla security, richiesta dal vertice, è la scintilla



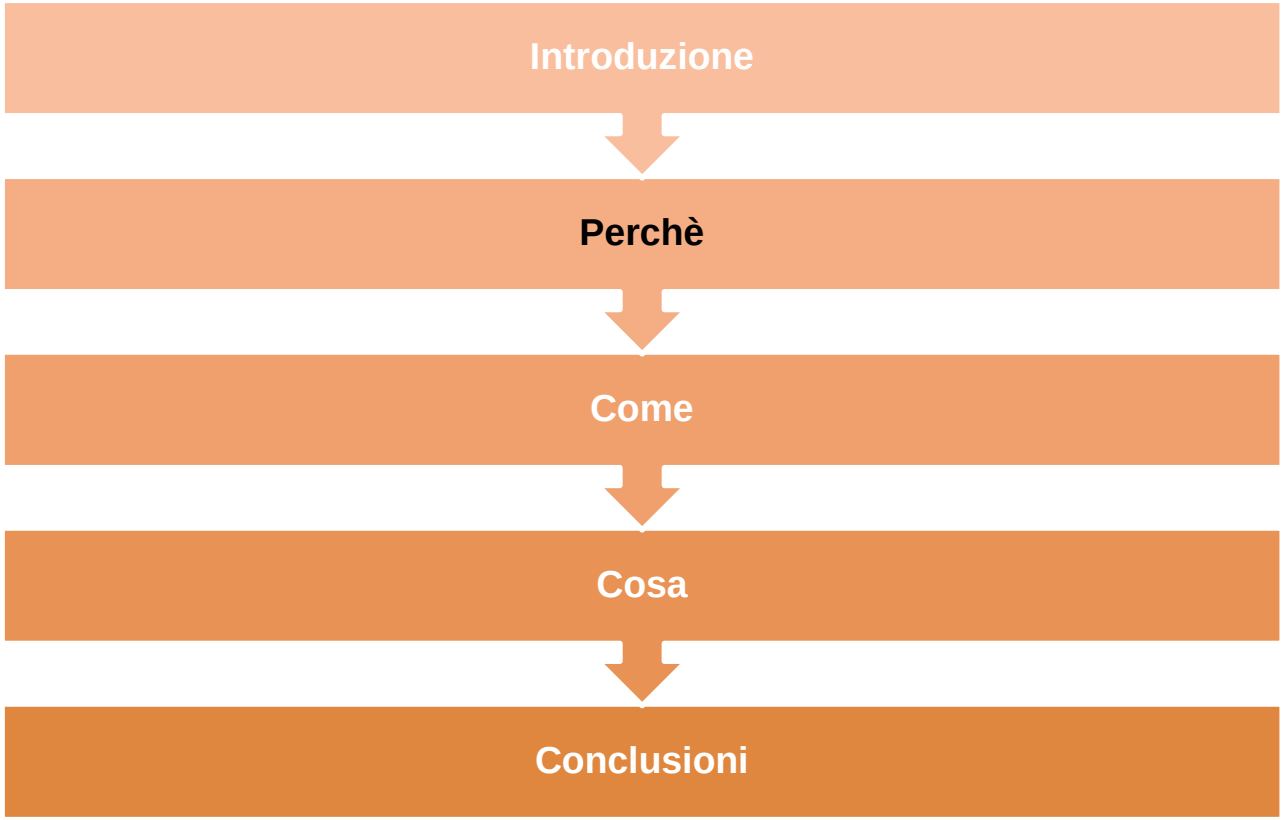
- Ha bisogno di chiarire / garantire agli azionisti, la “solidità tecnologica” dei processi di business e la corretta allocazione / efficienza dei budget > aka: redditività
- Ha bisogno di tradurre il concetto di “solidità tecnologica” in numeri. In altre parole aka: KPI
- Ha bisogno di individuare percorsi brevi, efficienti, per misurare e migliorare i KPI
- Ha bisogno di attuare le scelte tecnologiche ed organizzative per migliorare i KPI

L’impatto della tecnologia sul business può spiegare questa richiesta

Introduzione

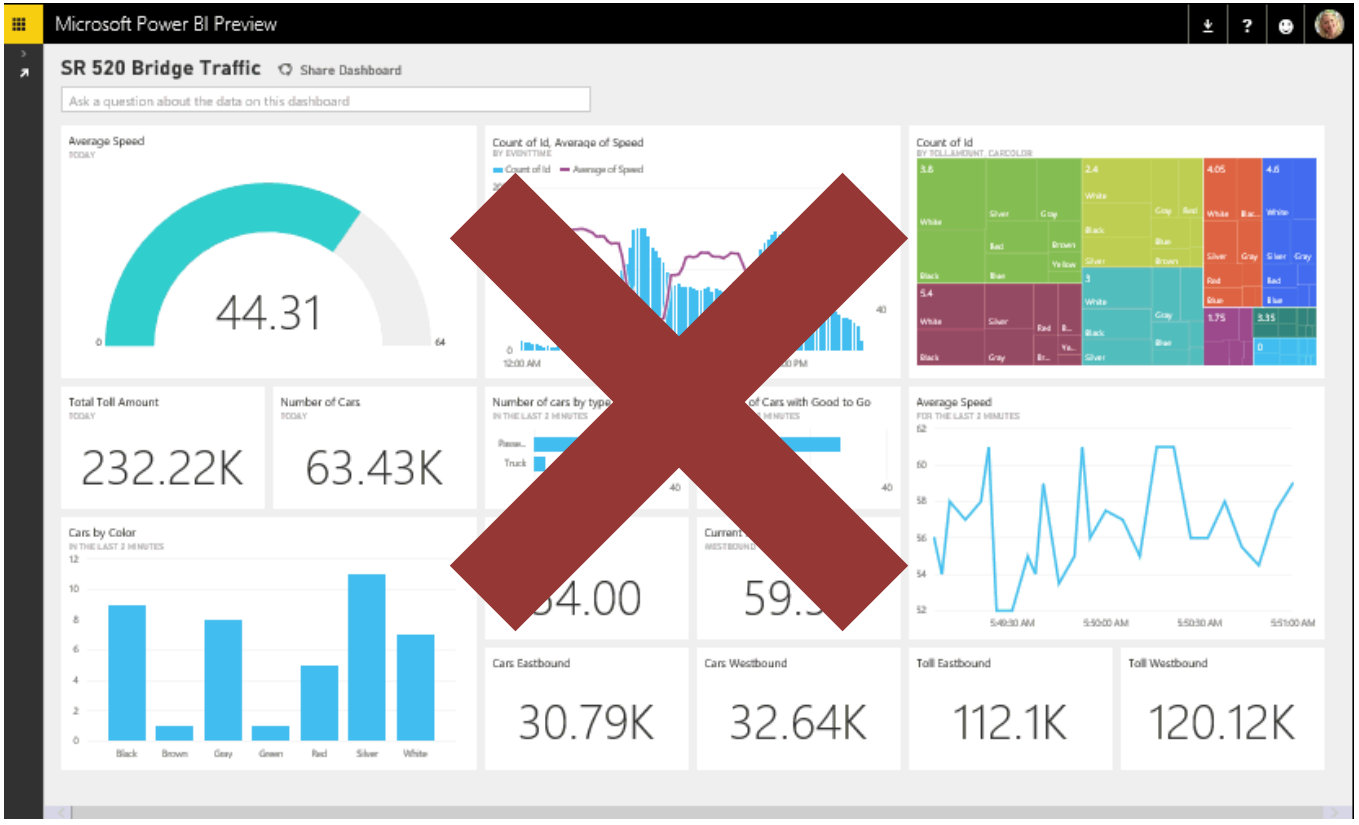
Source: “the state of consumer fintech”

Agenda



Avere un oggetto di design?

Perchè

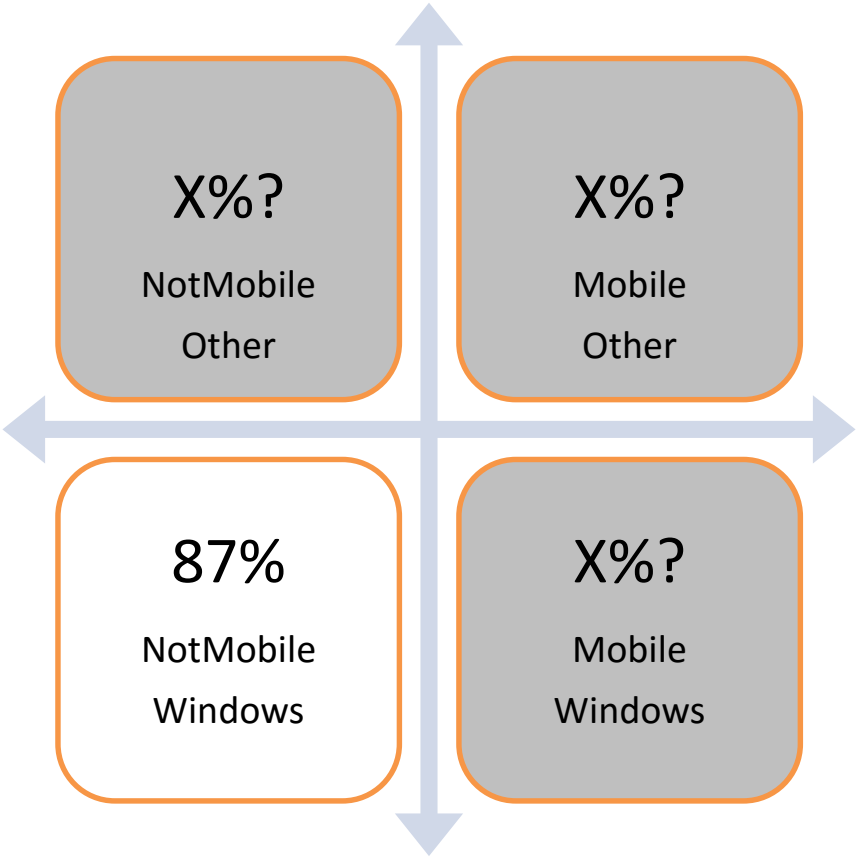


Avere una sintesi perfetta?

Perchè

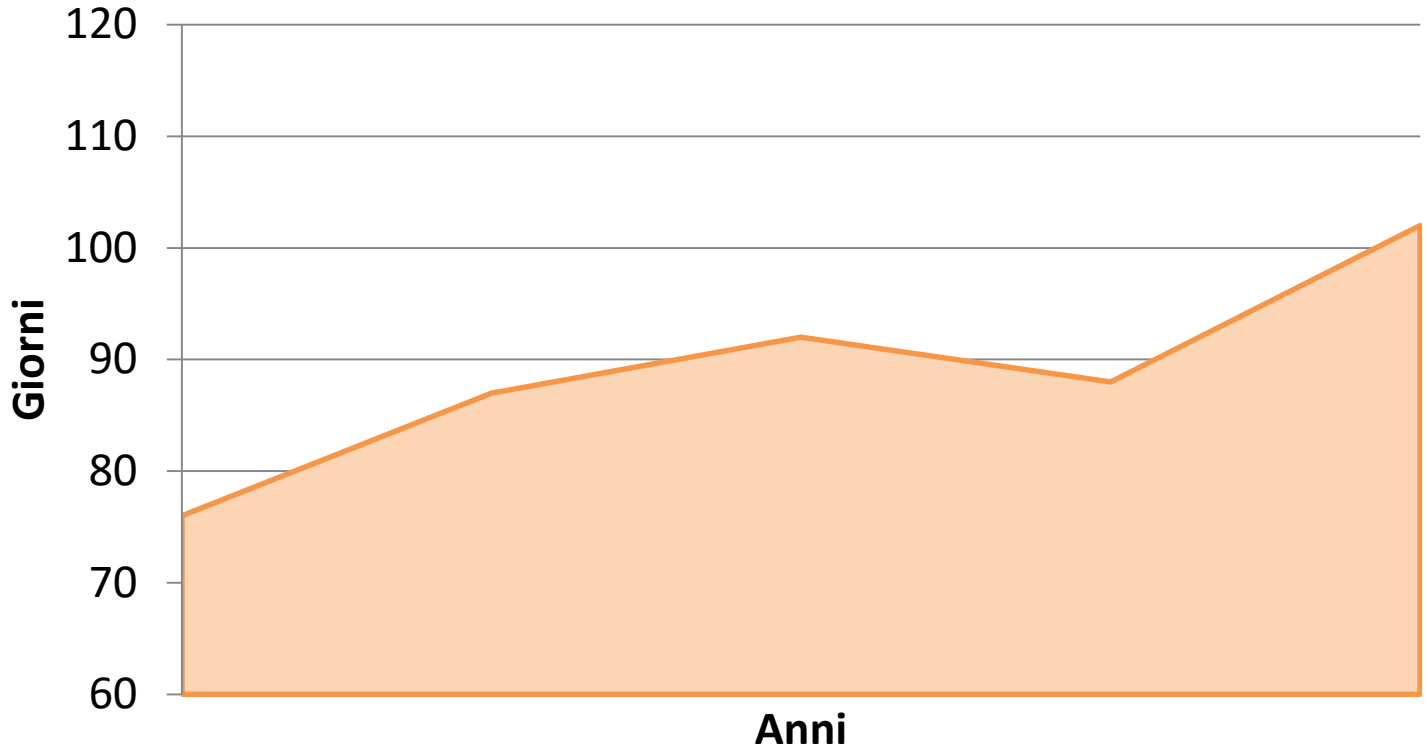
Scoprire che lo scope dell'antivirus potrebbe essere da allargare?

Perchè

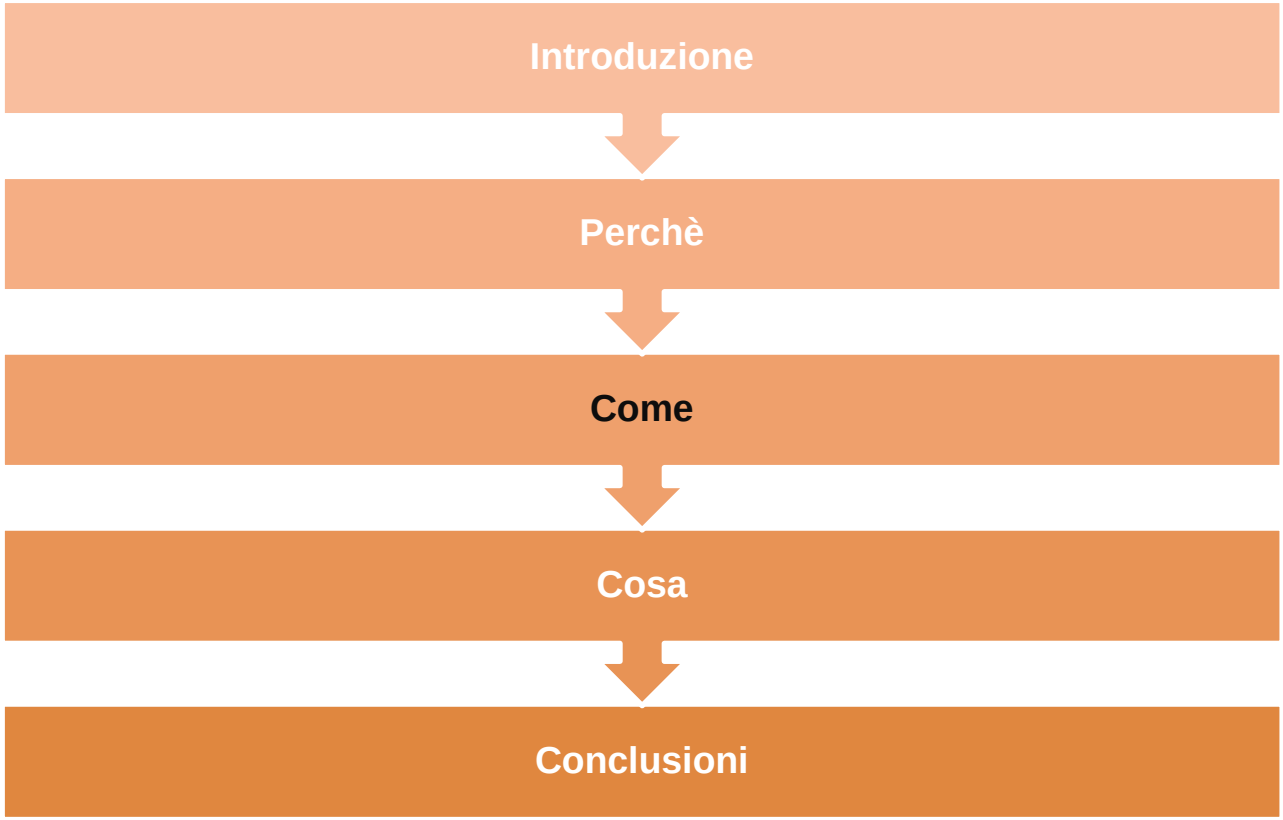


Scoprire che i tempi per un'azione di remediation sono da ridurre?

Perchè



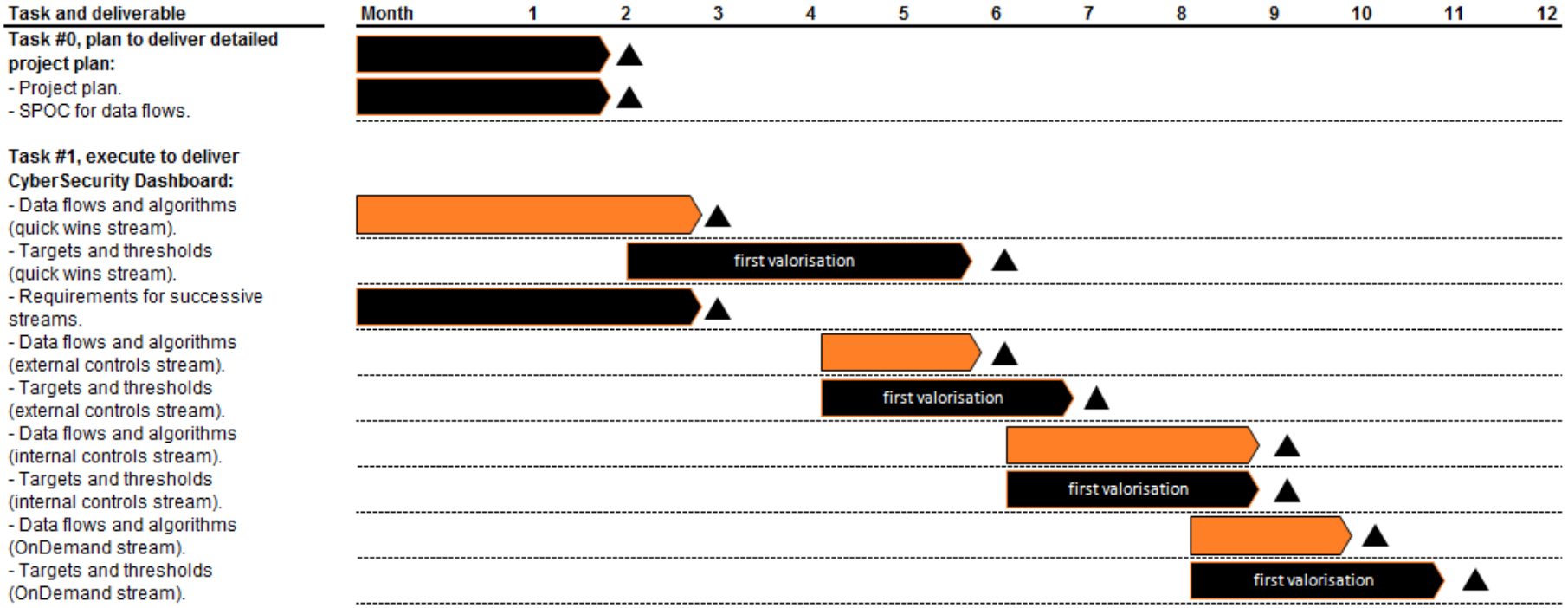
Agenda



Realizzare flussi dati e soglie credibili è la maggior parte del lavoro

Come

Project plan



Un tool di BI già conosciuto in azienda è meglio di “analysis paralysis”

Come

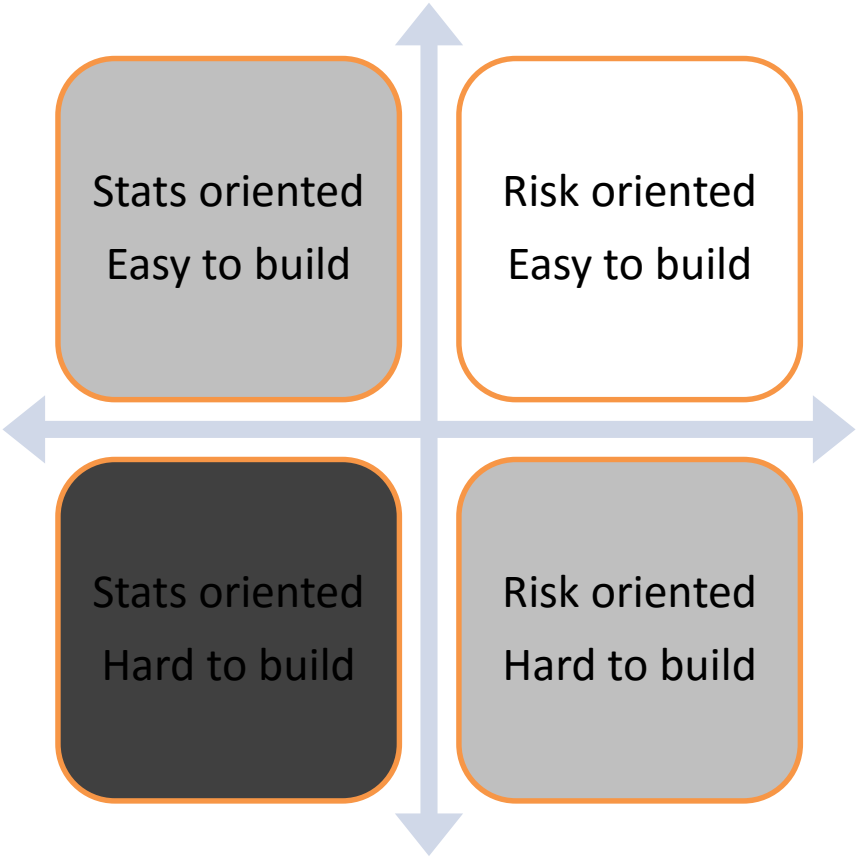
Source: Gartner

Meglio la ISO/IEC 27001 o la PCI-DSS che il Sacro Graal degli indicatori

Come

Scelta la struttura, concentrarsi su KPI che esprimono rischi

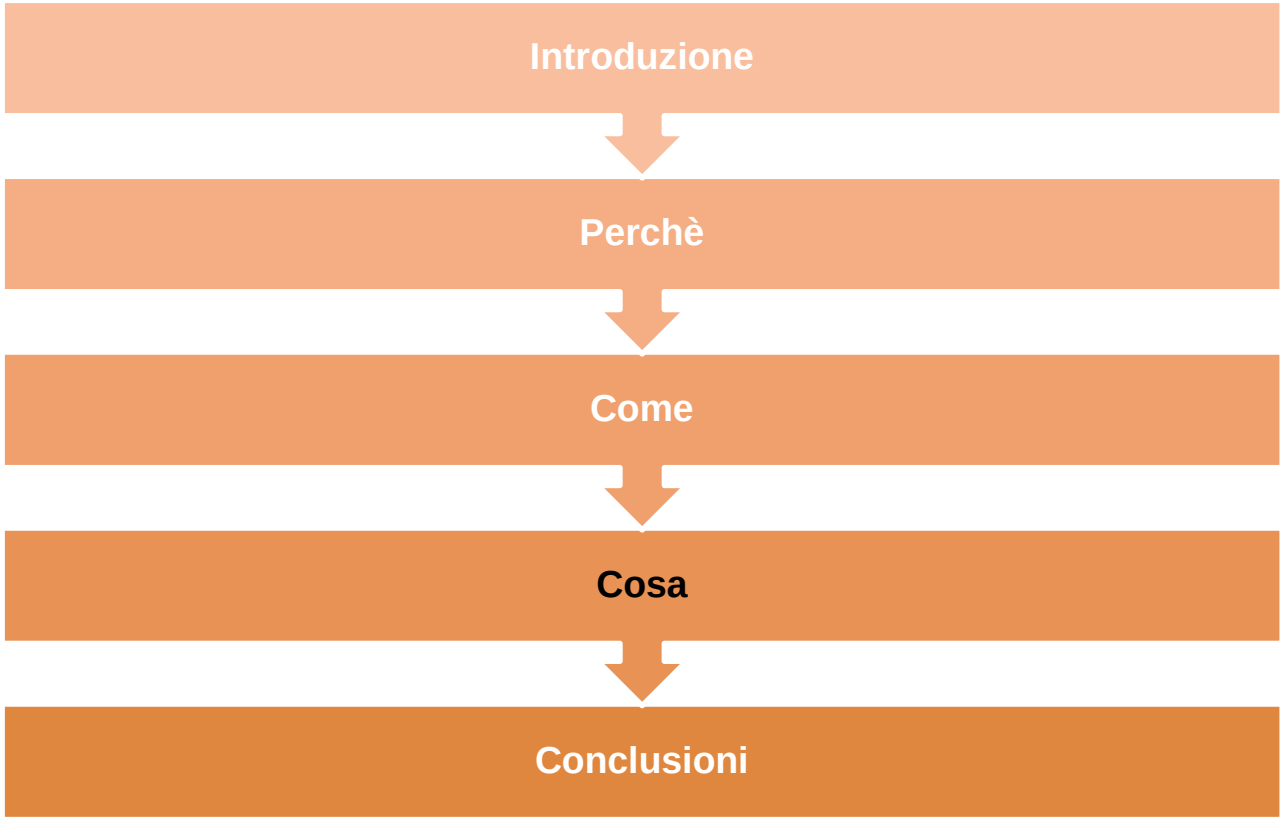
Come



Da realizzare passo dopo passo in una marcia costante

Come

Agenda



Il risultato tangibile è un tool di analytics. Ma è più importante…

Cosa

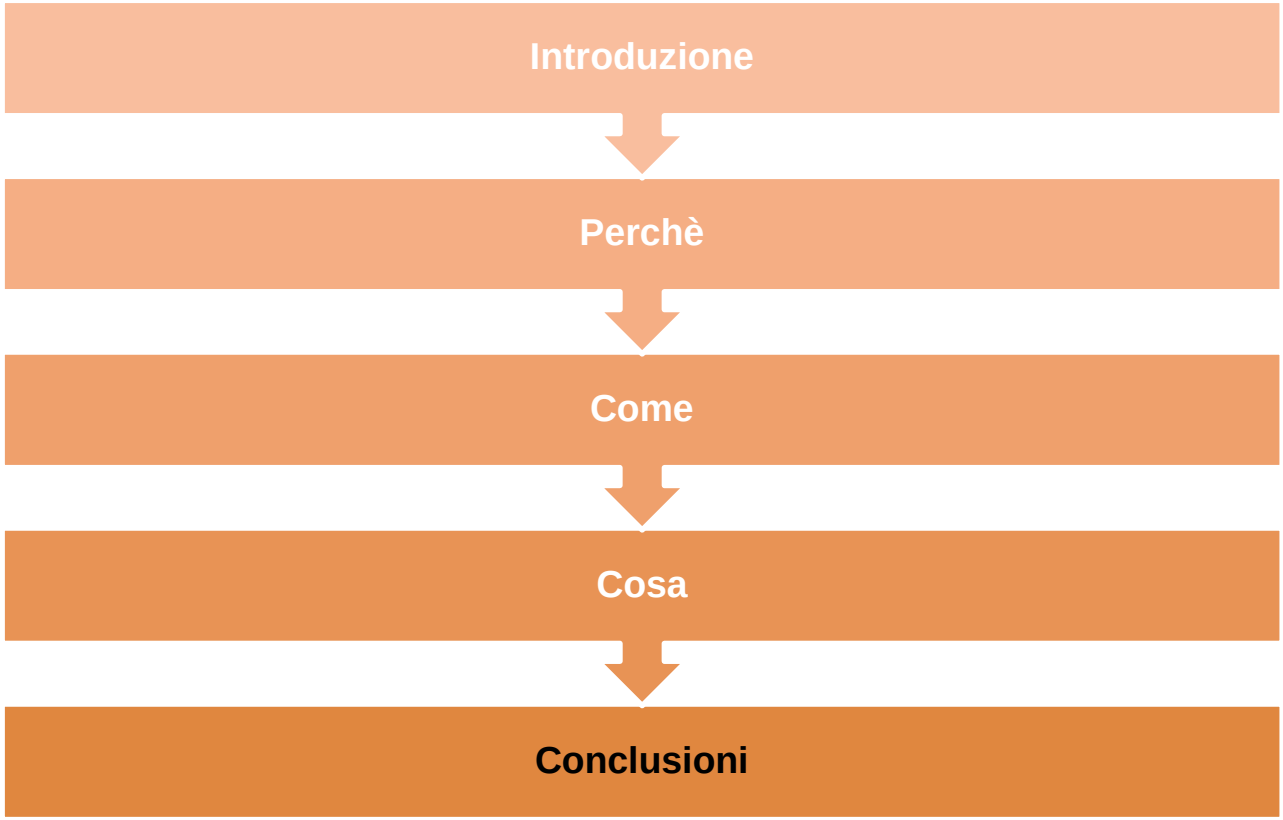
CYBERSECURITY DASHBOARD

INFORMATION SECURITY POLICIES	75%	🟢	↑
ORGANIZATION OF INFORMATION SECURITY	2%	🟡	→
HUMAN RESOURCE SECURITY	65%	🔴	↓
ASSET MANAGEMENT	40%	🟢	↑
ACCESS CONTROL	57%	🔴	→
CRYPTOGRAPHY	66%	🔴	↓
PHYSICAL AND ENVIROMENTAL SECURITY	10%	🟡	↑
OPERATIONS SECURITY	98%	🟡	→
COMMUNICATIONS SECURITY	9%	🟢	↓
SYSTEM ACQUSITION, DEVELOPMENT AND MAINTENANCE	40%	🔴	↑
SUPPLIER RELATIONSHIPS	75%	🔴	→
INFORMATION SECURITY INCIDENT MANAGEMENT	70%	🟢	↓
BUSINESS CONTINUITY	27%	🔴	↑
COMPLIANCE	92%	🟢	→

… L’aspetto intangibile. La consapevolezza che si ha ciò che si misura

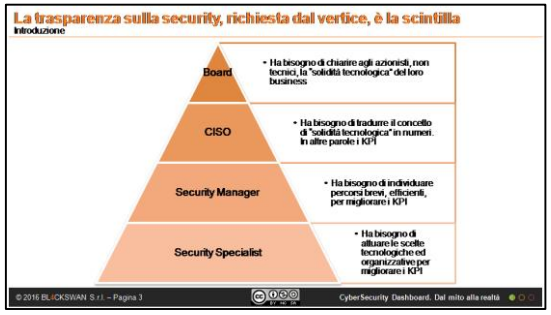
Cosa

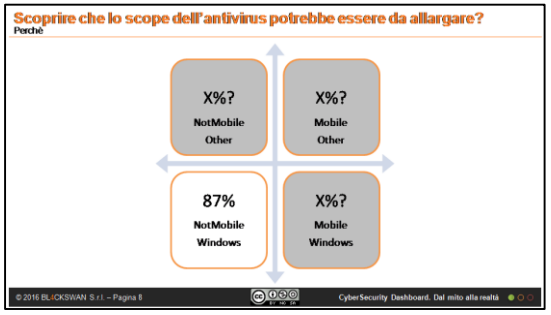
Agenda



In God we trust, all others must bring data *that represent risks*

Conclusioni





La tecnologia, presente nel core business, pone la cybersecurity al centro dell'interesse del Vertice

Affidarsi ad oggetti di design, sintesi perfette o cercare il Sacro Graal degli indicatori può costare tempo

Usare subito KPI che esprimono rischi come la bassa copertura dell'AV per ridurre rischi sottovalutati

CASE 1

APPLICAZIONE IN AMBITO ASSICURATIVO – CREAZIONE POLIZZA CYBER

OBIETTIVO

Valutare il livello di rischio effettivo in fase pre assuntiva.

COME

- Defininizione di una metodologia di analisi in linea con le esigenze di business e le tempistiche operative delle fasi preassuntive;
- Identificazione di un set di indicatori (singoli e aggregati) significativi per la definizione del rischio, del pricing e delle coperture assicurative

FASI PROGETTUALI

DEFINIZIONE METODOLOGIA	SCELTA INDICATORI	POC SU CLIENTI SELEZIONATI
TEAM MULTIDISCIPLINARE • UNDERWRITER • RISK • COSTING • LEGAL • ICT VISIONI DIVERGENTI	ADATTABILI A DIVERSI CONTESTI OPERATIVI ADATTABILI A DIVERSE INDUSTRY CHIUSI FACILMENTE MISURABILI SIGNIFICATIVI	IDENTIFICAZIONE DI AREE «COMUNI» POCO PRESIDIATE. DIFFICOLTA' DI IDENTIFICAZIONE DEL REFERENTE CORRENTO LATO «CLIENTE» SEMPLIFICAZIONE & REVISIONE DI ALCUNI INDICATORI DATI PER «SCONTATI»

BUSINESS VIEW X RISK - TECHNICAL VIEW

INDICATORI SINTETICI X **INDICATORI DETTAGLIO**

10na 100io → INDICATORI ASSOLUTI

INDICATORI SINTETICI — INDICATORI PUNTUALI → FASCE DI TOLLERANZA

CASE 2
APPLICAZIONE PER VALUTAZIONE FORNITORE P.A.

OBIETTIVO

Valutare il livello di sicurezza delle forniture acquisite da capitolato di Gara e Capitolato Tecnico

COME

- Defininizione della metodologia di valutazione
- Identificazione degli indicatori da analizzare in conformità a:
  - Capitolato di gara
  - Best Practice di Sicurezza
  - Hardening Guidelines

FASI PROGETTUALI

METODOLOGIA DI VALUTAZIONE

TEAM MULTIDISCIPLINARE
- LEGAL
- PROCUREMENT
- ICT
- OPERATION

SCELTA INDICATORI

SPECIFICI PER REQUISITO
SPECIFICI PER TECNOLOGIA ANALIZZATA
SPECIFICI PER PROCESSO ANALIZZATO

ANALISI INTERNA

- VALUTAZIONE EFFETTIVA DEI PRESIDI DI SICUREZZA IMPLEMENTATI A LIVELLO TECNICO
- VALUTAZIONE COMPLESSIVA DELLA SICUREZZA DEI PROCESSI DI BUSINESS
- IDENTIFICAZIONE DELLE VIOLAZIONI CONTRATTUALI
- VALUTAZIONE DELLE PENALI APPLICABILI
- VALUTAZIONE DEL PIANO DI RIENTRO DA PARTE DEL FORNITORE

INDICATORI PUNTUALI

200 circa

ESTENSIONE A TUTTE LE LINEE DI FORNITURA