Security Summit

Verona, 24 ottobre 2024

Una Compliance più gestibile con l'automazione dei Controlli di Sicurezza

Paolo Francesco Lenti | Head of CRU (Cyber Response Unit)

Sala Kandinsky | 24 ottobre 2024 | 12:20 - 13:00

Luca Bechelli

Comitato scientifico

Partner @p4i – gruppo digital360

Paolo Francesco Lenti

Head of CRU - Cyber Response Unit

deda.cloud

deda.cloud
YOUR SAFE IT

CRU – cosa succede?

Team di sicurezza sotto organico:
Rispetto all'anno precedente, un numero maggiore di organizzazioni (+26%) ha dovuto far fronte a gravi carenze di personale, con una media di 1,76M$ di costi extra in caso di incidenti.

La prevenzione alimentata dall'intelligenza artificiale paga:
Due organizzazioni su tre stanno implementando l'intelligenza artificiale e l'automazione della sicurezza nel loro SOC. Quando utilizzata in modo estensivo nei flussi di lavoro di prevenzione, le organizzazioni hanno risparmiato una media di 2,2M$ in caso di data breach.

Lacune nella visibilità dei dati:
Il 40% delle violazioni ha riguardato dati archiviati in più ambienti, tra cui cloud pubblico, cloud privato e on-premise, con un incremento >5M$ di costi ed hanno richiesto più tempo per essere identificate e arginate (283 giorni).

Fonte: 2024 IBM Security Cost of a Data Breach

CRU – notiziario 2024

Credenziali rubate in cima ai vettori di attacco iniziali:
Con il 16%, le credenziali rubate/compromesse sono state il vettore di attacco iniziale più usato, con quasi 10 mesi necessari per identificarlo.

Le infrastrutture critiche ed i costi di violazione elevati:
Le organizzazioni che si occupano di sanità, servizi finanziari, industria, tecnologia ed energia hanno sostenuto i costi di violazione più elevati in tutti i settori, con costi medi di violazione pari a 9,7M$.

Costi della violazione trasferiti ai consumatori:
Il 63% delle organizzazioni ha dichiarato che quest'anno aumenterà il costo di beni o servizi a causa di violazioni.

Meno riscatti pagati con le forze dell'ordine ingaggiate:
Coinvolgendo le forze dell'ordine, le vittime di ransomware hanno risparmiato in media quasi 1M$ in costi di violazione, 63% di loro sono state anche in grado di evitare il pagamento di un riscatto.

Fonte: 2024 Security Report CLUSIT ed IBM Security Cost of a Data Breach

NIS2 e DORA: cosa succede(rà)… To do list

Valutazione e gestione del rischio come cultura:

- Effettuare valutazioni e mitigazione del rischio più dettagliate relative ai sistemi aziendali, nonché di quelli di fornitori terzi.
- Implementare piani di continuità operativa e di disaster recovery più solidi.
- Implementare procedure di controllo continuo della compliance.

Segnalazione degli incidenti, sì ma strutturata:

- Stabilire procedure standard e tempistiche più rigide per la segnalazione degli incidenti sia ai clienti che alle autorità di regolamentazione, collegate ad un piano di risposta agli incidenti di sicurezza.

Gestione del rischio di terzi:

- Rivedere le procedure di due diligence rafforzandole, per la selezione di fornitori e subappaltatori, includendo requisiti contrattuali che impongano alle terze parti di soddisfare gli standard DORA/NIS2.

Test di resilienza:

- Condurre periodicamente penetration test e “Red-Team exercises”.
- Simulare scenari realistici di attacco cyber per testare le capacità di risposta.

NIS2 e DORA: *adattarsi alla nuova normalità*

Pianificazione proattiva della conformità:

- Sviluppare una piano di attuazione per soddisfare i requisiti di DORA e NIS2.
- Assegnare responsabilità chiare all'interno dell'organizzazione per l'esecuzione del piano di conformità, con tempi e qualità misurabili e certi.

Miglioramento continuo:

- Stabilire una forte cultura della sicurezza, non solo informatica.
- La sicurezza informatica è responsabilità di ogni dipendente.

Guardare avanti:

- Costruire un ecosistema di sicurezza collaborativo con clienti e partner per garantire la resilienza delle terze parti.
- Impegnarsi con i gruppi di settore e le autorità di regolamentazione per rimanere informati sull'evoluzione dei requisiti e delle best practice.

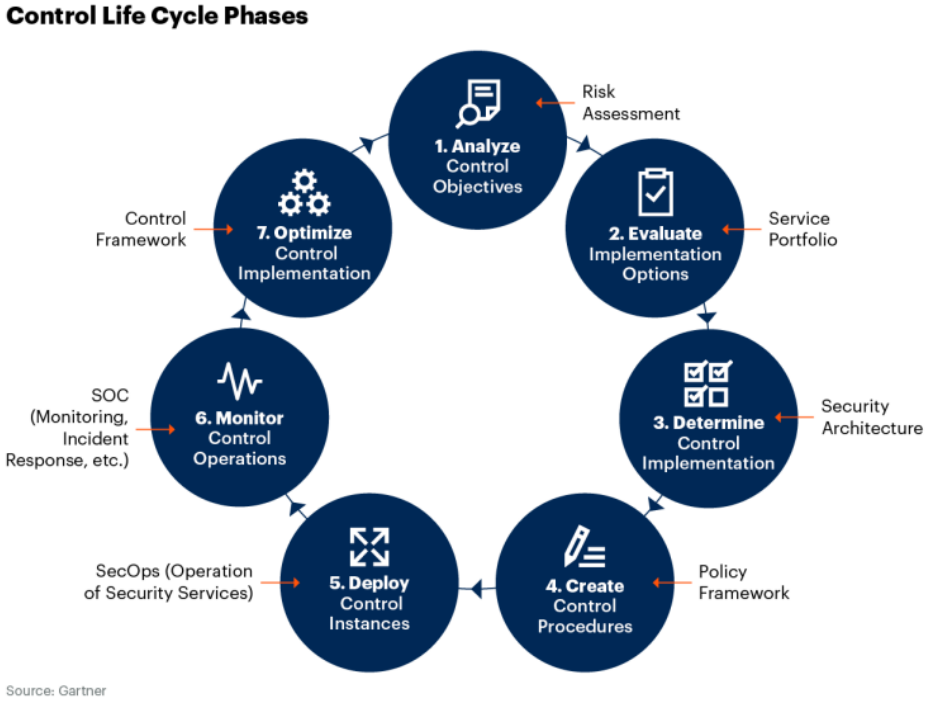
Non si tratta di una soluzione una tantum:

- DORA e NIS2 significano il passaggio a una mentalità più proattiva in materia di cybersecurity e il miglioramento continuo delle misure di protezione e risposta.

CCM: Continuous Control Monitoring

“Il **Continuous control monitoring (CCM)** è un insieme di tecnologie che automatizza il monitoraggio dell'efficacia dei controlli di cybersecurity e la raccolta di informazioni rilevanti in tempo quasi reale.“

Fonte: Gartner

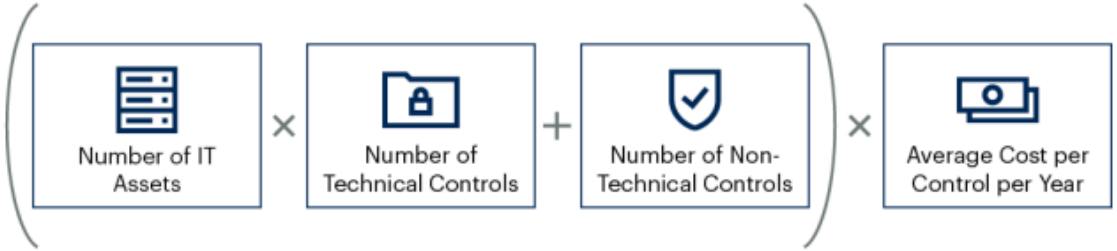


CCM: Cosa prevede il controllo del rischio?

- I controlli derivano da standard di sicurezza, quadri normativi, obblighi normativi e politiche interne.
- È necessario testare e monitorare regolarmente i controlli per garantirne l'efficacia e la conformità.
- Questo lavoro non solo è spesso oneroso, ma poiché in genere viene svolto in modo manuale e frammentario, è soggetto a errori e incompletezze e spesso non riutilizzabile.

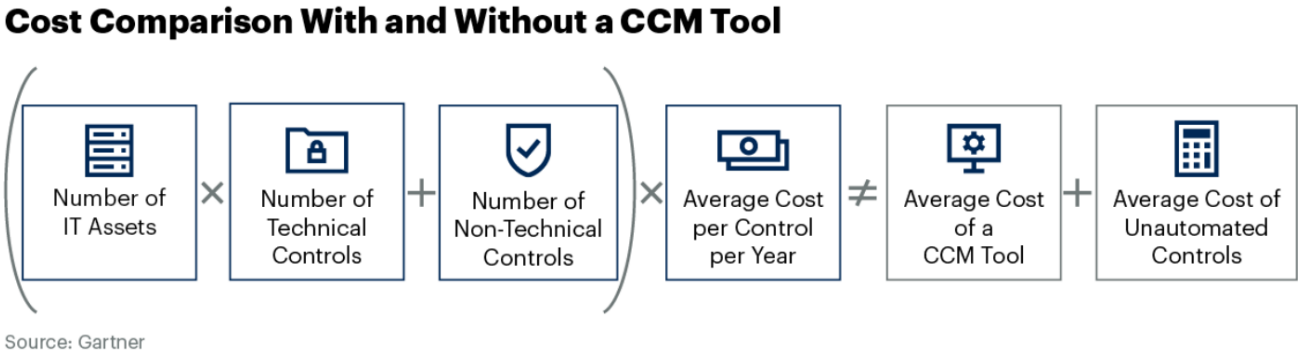
Il costo annuale della gestione dei controlli può essere stimato approssimativamente:

Estimation of Annual Cost of Security Control Management for SRM Leaders



Source: Gartner

CCM: Cosa cambia con il controllo automatizzato?

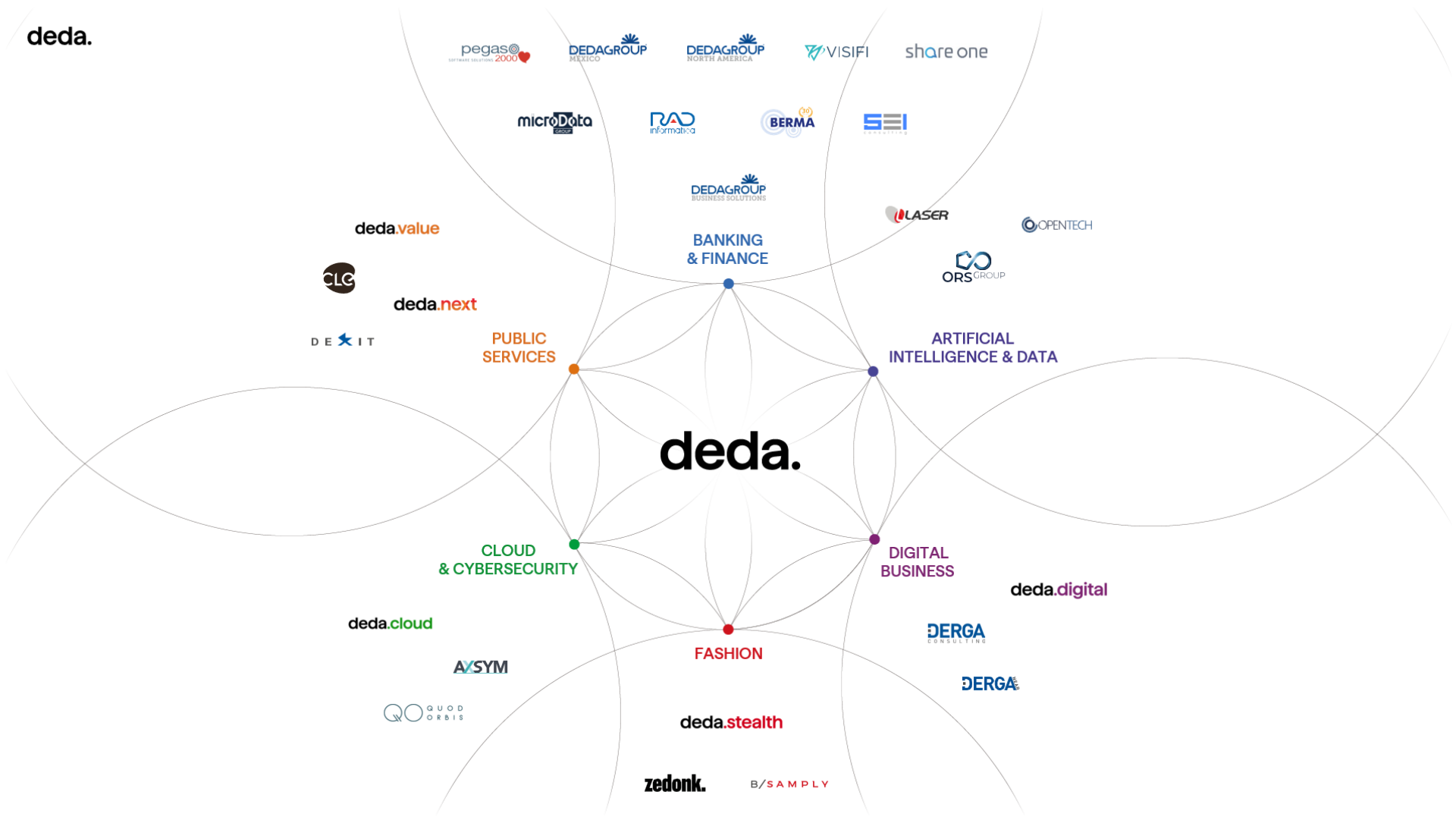


- Gli strumenti CCM offrono ai Risk Manager ed ai relativi team operativi IT la possibilità di automatizzare e pianificare i controlli, tramite il supporto delle attività durante il ciclo di vita della gestione dei controlli:

- la raccolta di dati da diverse fonti, la verifica dell'efficacia dei controlli, la rendicontazione dei risultati, gli avvisi da fonti diverse, la comunicazione dei risultati, l'avviso agli stakeholder e l'attivazione di azioni correttive in caso di controlli inefficaci o anomalie.

Quod Orbis: cosa può fare una piattaforma CCM?

- ***Tracciare e segnalare le performance dei controlli*:** colleziona, normalizza e correla i dati sulle prestazioni dei controlli per ottenere visibilità sulle prestazioni e le tendenze dei controlli stessi.
- ***Identificare le lacune sui controlli*:** crea e compara la baseline dei controlli prescritti e la confronta con l'implementazione effettiva.
- ***Supportare l'audit di sicurezza*:** fornisce prove per la valutazione dell'aderenza ai controlli, alle politiche ed alle procedure previste e prescritte.
- ***Mantenere la conformità alle normative e agli standard di settore*:** fornisce prove che dimostrino l'aderenza ai requisiti di conformità della sicurezza derivanti dagli standard di settore, nonché alle norme, ai regolamenti e alle leggi richieste dai governi o dagli enti normativi.
- ***Monitorare il rischio cyber*:** fornisce informazioni quasi in tempo reale per le attività di valutazione del rischio che esaminano la criticità dei vari Sistemi e degli accessi degli utenti.
- ***Migliorare l'efficienza operative della sicurezza*:** integra la capacità dell'organizzazione di far fronte alle minacce alla sicurezza.


deda.
pegaso 2000
DEDAGROUP MEXICO
DEDAGROUP NORTH AMERICA
VISIFI
share one
microData group
RAD informatica
BERMA
SEI
DEDAGROUP BUSINESS SOLUTIONS
deda.value
BANKING & FINANCE
LASER
OPENTECH
CLC
ORS GROUP
deda.next
DE IT
PUBLIC SERVICES
ARTIFICIAL INTELLIGENCE & DATA
deda.
CLOUD & CYBERSECURITY
DIGITAL BUSINESS
deda.digital
deda.cloud
DERGA CONSULTING
FASHION
AXSYM
DERGA
QUOD ORBIS
deda.stealth
zedonk.
B/SAMPLY

QUOD ORBIS

https://www.quodorbis.com/

Award winning, Gartner recognised, purpose built Continuous Controls Monitoring (CCM) platform and service.

- Founded in 2018
- ~27 staff
- UK headquarters
- Global customer base
- Managed platform offered on AWS & Deda Cloud

- Acquired by Deda in May 2024

> “ Continuous controls monitoring (CCM) automates the monitoring of cybersecurity controls’ effectiveness and relevant information gathering in near real time. ”
>
> - Gartner

deda.

Gartner

Q&A

GRAZIE

https://deda.cloud
info@dedagroup.it

servizi