DIRETTIVA NIS2:
IL CONTO ALLA ROVESCIA È INIZIATO

CYBEROO

LUCA BENATTI

BUSINESS DEVELOPMENT MANAGER
CYBEROO

DIRETTIVA NIS2: PILASTRO DELLA CYBER RESILIENCE EUROPEA

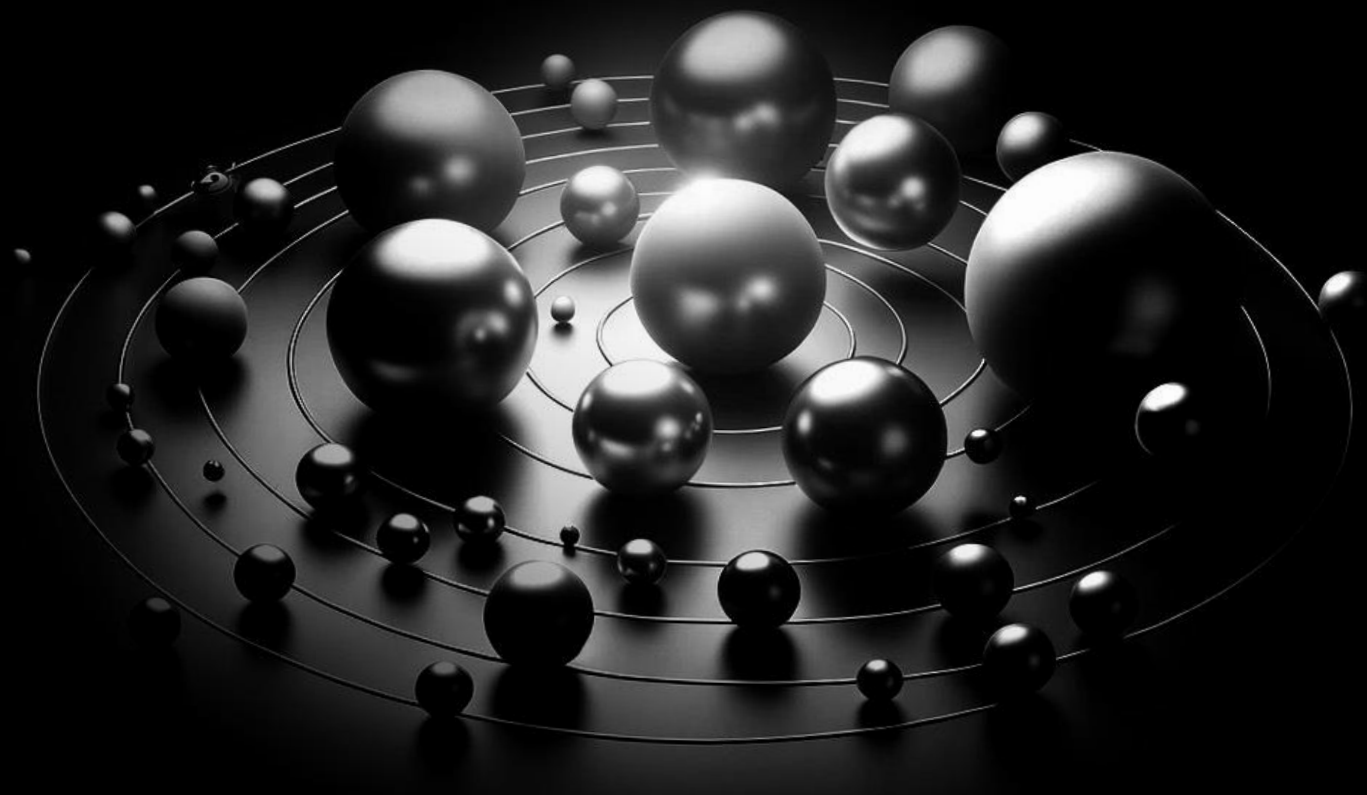
La NIS2 è l'aggiornamento della Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi, mirata a rafforzare la cyber resilience delle infrastrutture critiche in tutta l'UE per garantire un livello comune elevato di cybersicurezza e migliorare il funzionamento del mercato interno.

GESTIONE DELLA SUPPLY CHAIN

I **fornitori terzi** possono rappresentare una grande minaccia per la resilienza aziendale.

Il controllo della supply chain prevede la valutazione dei fornitori, la verifica dei loro processi di sicurezza e la stipula di accordi di livello di servizio (SLA) che definiscono le responsabilità in materia di sicurezza.

Un controllo rigoroso dei fornitori aiuta a mitigare il rischio di attacchi che sfruttano le loro vulnerabilità.



NIS: PERCHÉ È STATA NECESSARIA UNA REVISIONE?

La **Direttiva NIS** del 2016 richiedeva alle società di adottare misure per ridurre i rischi di cybersecurity. L'articolo 23 della direttiva sottolinea la necessità di **aggiornamenti continui**.

Per questo, la Commissione Europea ha deciso di aggiornare la direttiva a causa della crescente dipendenza dalla tecnologia negli ambienti lavorativi e non solo.

NIS2: OBIETTIVI PRINCIPALI

1

RESILIENZA

Aumentare il livello di resilienza informatica di un insieme di aziende che cooperano nell'Unione Europea con ruoli importanti per l'economia e la società.

2

RIDUZIONE INCOERENZE

Ridurre le incoerenze nella resilienza nel mercato interno nei settori già contemplati dalla direttiva.

3

MAGGIORE CONSAPEVOLEZZA

Adozione di misure per aumentare il livello di fiducia tra le autorità competenti con una condivisione maggiore di informazioni.

COSA SI INTENDE PER «INCIDENT»

QUASI INCIDENTE

Un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati ma che è stato efficacemente evitato o non si è verificato.

INCIDENTE

Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.

INCIDENTE DI CIBERSICUREZZA SU VASTA SCALA

Un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri.

GLI STEP PER LA COMPLIANCE

1

IMPLEMENTARE MISURE DI SICUREZZA ADEGUATE

Proteggere i propri sistemi e dati adottando adeguate misure tecniche e organizzative.

2

CONOSCERE GLI OBBLIGHI

Studiare attentamente i requisiti della NIS2 e valutare il proprio livello di conformità.

3

COLLABORARE CON L'AUTORITÀ NAZIONALE COMPETENTE

Instaurare una collaborazione con l’Autorità responsabile dell'applicazione della NIS2.

I RISCHI E LE SANZIONI

La Direttiva NIS2 si applica a un ampio spettro di aziende e organizzazioni, suddivise in due categorie: **essenziali** e **importanti**. Le aziende essenziali offrono servizi cruciali per la società e l'economia, mentre le aziende importanti, pur non fornendo servizi essenziali, sono rilevanti per il contesto economico e sociale.

Per le aziende **essenziali**, le sanzioni in caso di non conformità possono arrivare fino a 10 milioni di euro o al 2% del fatturato globale annuo precedente.

Per le aziende **importanti** le sanzioni possono raggiungere i 7 milioni di euro o un massimo di almeno l'1,4% del fatturato annuo globale.

SETTORI COPERTI DALLA DIRETTIVA NIS2

Energia	Trasporti	Settore bancario	Infrastrutture dei mercati finanziari
Settore sanitario	Acqua potabile	Acque reflue	Infrastrutture digitali
Gestione dei servizi TIC	Spazio	Servizi postali e di corriere	Gestione dei rifiuti
Fabbricazione, prod. e distr. di sostanze chimiche	Produzione, trasformazione e distribuzione di alimenti	Fabbricazione	Ricerca

DEADLINE NAZIONALI & ATTIVITÀ ANNUALI

DAL 01/01 AL 28/02 DI OGNI ANNO

I soggetti previsti si devono registrare o aggiornare la propria registrazione sulla piattaforma digitale dell'Autorità nazionale competente ACN.

ENTRO IL 31/03 DI OGNI ANNO

L'Autorità redige l'elenco dei soggetti essenziali e importanti sulla base delle registrazioni ricevute attraverso la piattaforma.

TRA IL 1° E 15/04 DI OGNI ANNO

Attraverso la piattaforma, l'ACN comunica ai soggetti registrati l'inserimento, la permanenza o l'espulsione nell'elenco dei soggetti importanti o essenziali.

DAL 15/04 AL 31/05 DI OGNI ANNO

Le aziende notificate devono aggiornare le informazioni su: IP pubblici, nomi di dominio, stati membri di distribuzione e responsabili della sicurezza.

DEADLINE NAZIONALI & ATTIVITÀ ANNUALI

A PARTIRE DAL 1° GENNAIO 2026

Si dovrà adempire all’obbligo di notifica degli incidenti. Questo richiede come minimo di stabilire il processo di gestione degli incidenti.

ENTRO IL 1° OTTOBRE 2026

Adempiere agli obblighi degli organi di amministrazione e direttivi: in materia di misure di sicurezza, raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio, laddove applicabile.

OBBLIGO DI NOTIFICA DEGLI INCIDENTI

Le Entità essenziali e importanti dovranno:

1. **ENTRO 24 ORE – inviare una prenotifica**, per comunicare che i soggetti sono venuti a conoscenza dell'incidente significativo, inoltre **ENTRO 24 ORE** si dovrà effettuare la **comunicazione dell'incidente a ACN**
2. **ENTRO 72 ORE – inviare una notifica dell'avvenimento**
3. **UNA EVENTUALE RELAZIONE INTERMEDIA**, su richiesta di CSIRT Italia
4. **ENTRO UN MESE DALLA TRASMISSIONE DELLA NOTIFICA** - una eventuale relazione finale

GESTIONE COORDINATA INCIDENT	**SCAMBIO INFORMAZIONI**	**MISURAZIONI COSTANTI**

COOPERAZIONE TRA GLI STATI MEMBRI UE

Il compito di **EU-CyCLONe** sarà di sostenere la gestione coordinata degli incidenti di cybersicurezza in tutta l'UE, oltre a garantire il **regolare scambio di informazioni** e rafforzare il flusso di informazioni interne cooperando con la rete dei CSIRT.

Per contribuire allo sviluppo della fiducia e promuovere una cooperazione operativa rapida ed efficace tra gli Stati membri, è istituita una **rete di CSIRT nazionali**. La rete garantisce lo scambio di informazioni su incident, assiste gli stati membri e stila un report ogni 24 mesi.

L'ENISA ogni due anni dovrà fare un report sulla situazione di sicurezza dell'EU.

Gli stati membri potranno richiedere a Entità Essenziali e Importanti di certificare prodotti, servizi e processi ICT specifici.

GESTIONE COORDINATA INCIDENT	**SCAMBIO INFORMAZIONI**	**MISURAZIONI COSTANTI**

STRATEGIE PER ELEVARE LE MISURE DI SICUREZZA AZIENDALE

1. **DISPORRE DI SISTEMI DI MONITORAGGIO E RISPOSTA H24**
   Dotarsi di un processo continuo in grado di rilevare attività sospette e rispondere in tempo reale.

2. **ANALIZZARE I RISCHI E POLITICHE DI SICUREZZA DEI SISTEMI INFORMATIVI**
   Esaminare i processi, le tecnologie, i rischi e implementare una strategia di cybersecurity.

3. **GESTIRE PRONTAMENTE GLI INCIDENTI**
   Disporre di un piano di risposta agli incidenti in grado di prevenire, individuare e rispondere.

4. **AVERE UN PIANO DI CONTINUITÀ E GESTIONE DELLE CRISI**
   Definire le procedure in caso di incidente per riprendere le attività nel minor tempo possibile.

NIS2 VS. ISO 27001

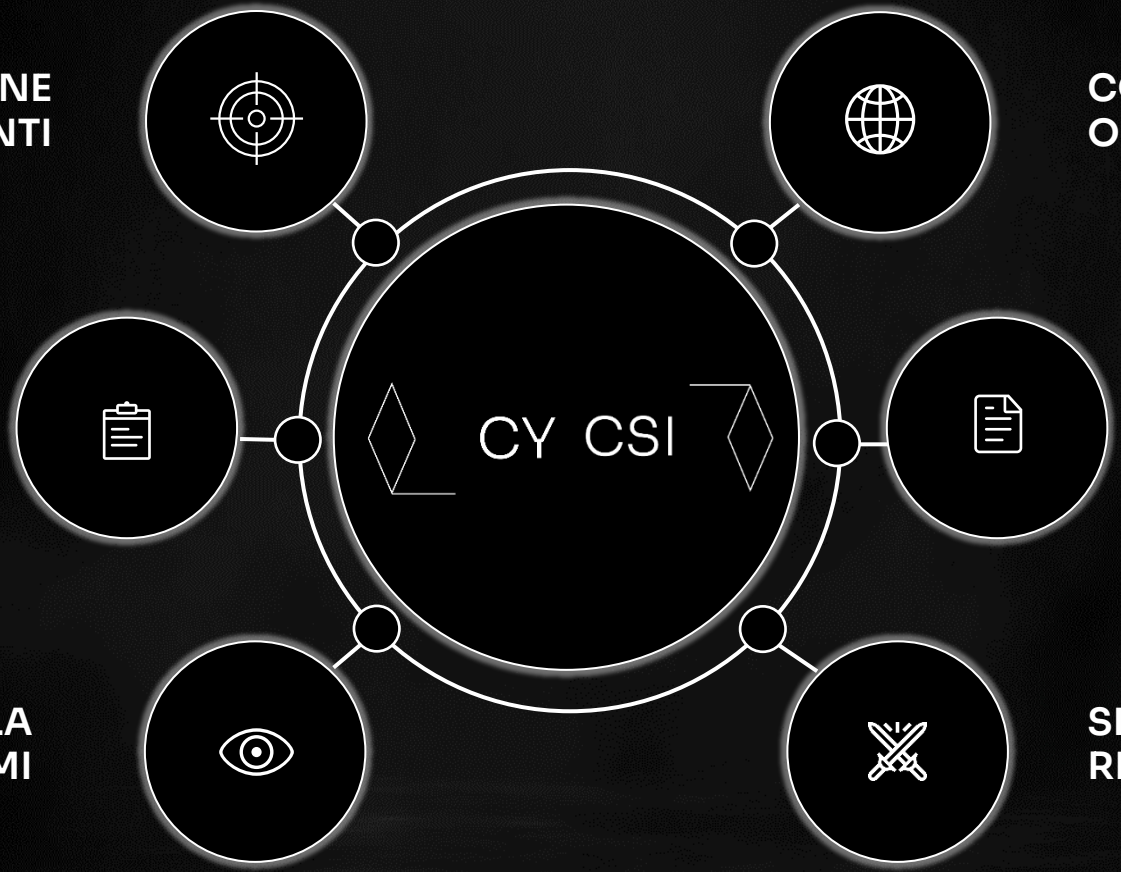
	DIRETTIVA NIS2	ISO 27001
APPROCCIO	Obbligatorio per settori critici	Volontario
FOCUS	Gestione del rischio di cyber incidenti	Sicurezza delle informazioni in generale
REQUISITI	Specifici e prescrittivi	Flessibili e adattabili
COMPLIANCE	Sanzioni per la non conformità	Certificazione volontaria

È ORA DI AGIRE.
LA **CYBERSECURITY**
NON SI DISCUTE, SI FA.

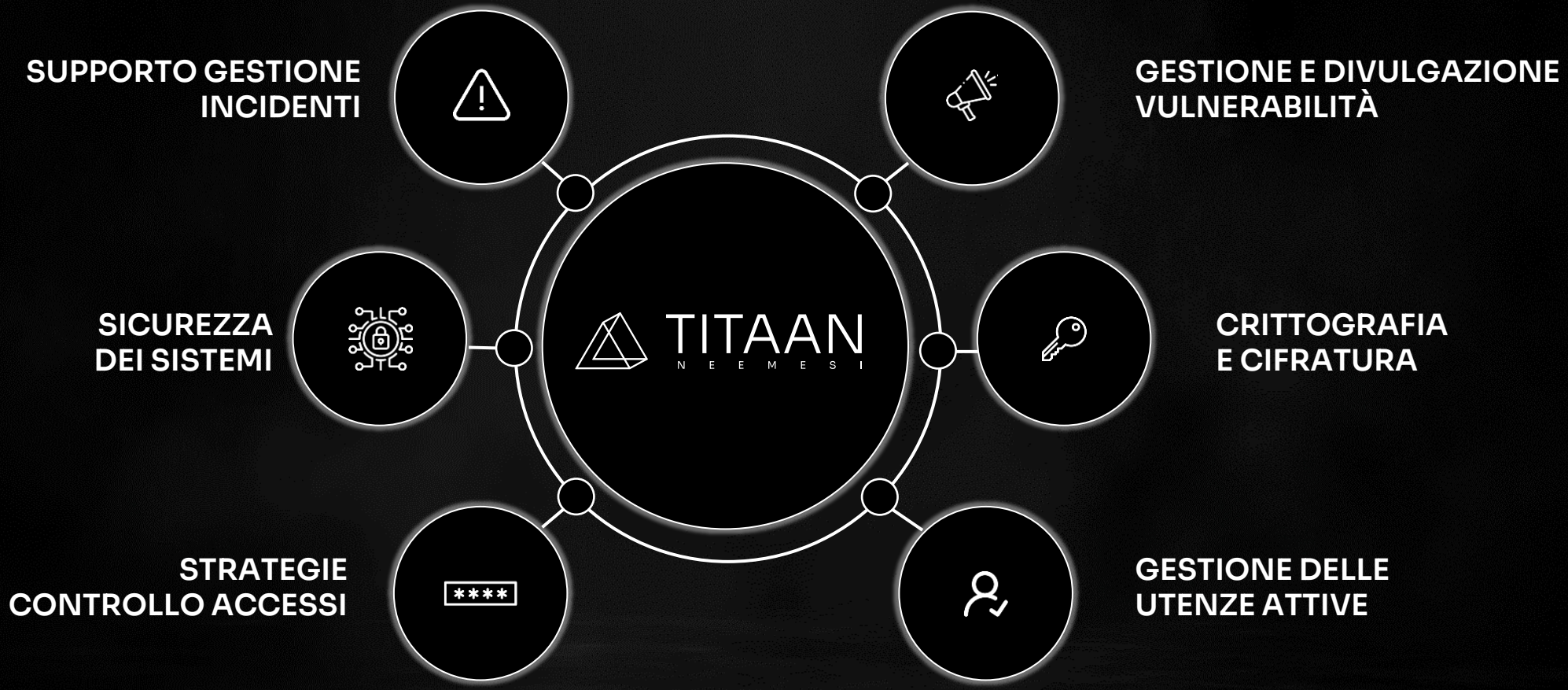
CYBEROO PER LA NIS2

1. Analisi dei **rischi** e **politiche di sicurezza** dei sistemi informativi
2. **Gestione degli incidenti** (prevenzione, individuazione e risposta agli incidenti)
3. **Continuità operativa** e gestione delle **crisi**
4. Sicurezza della **catena di approvvigionamento**
5. Sicurezza della **rete** e dei **sistemi**, compresa la gestione e divulgazione delle **vulnerabilità**
6. Politiche e procedure per valutare **l'efficacia della gestione dei rischi**
7. Sicurezza delle **risorse umane**, strategie di controllo dell'accesso e gestione degli attivi
8. **Comunicazione** a fornitori e clienti quando l'incidente è in corso.

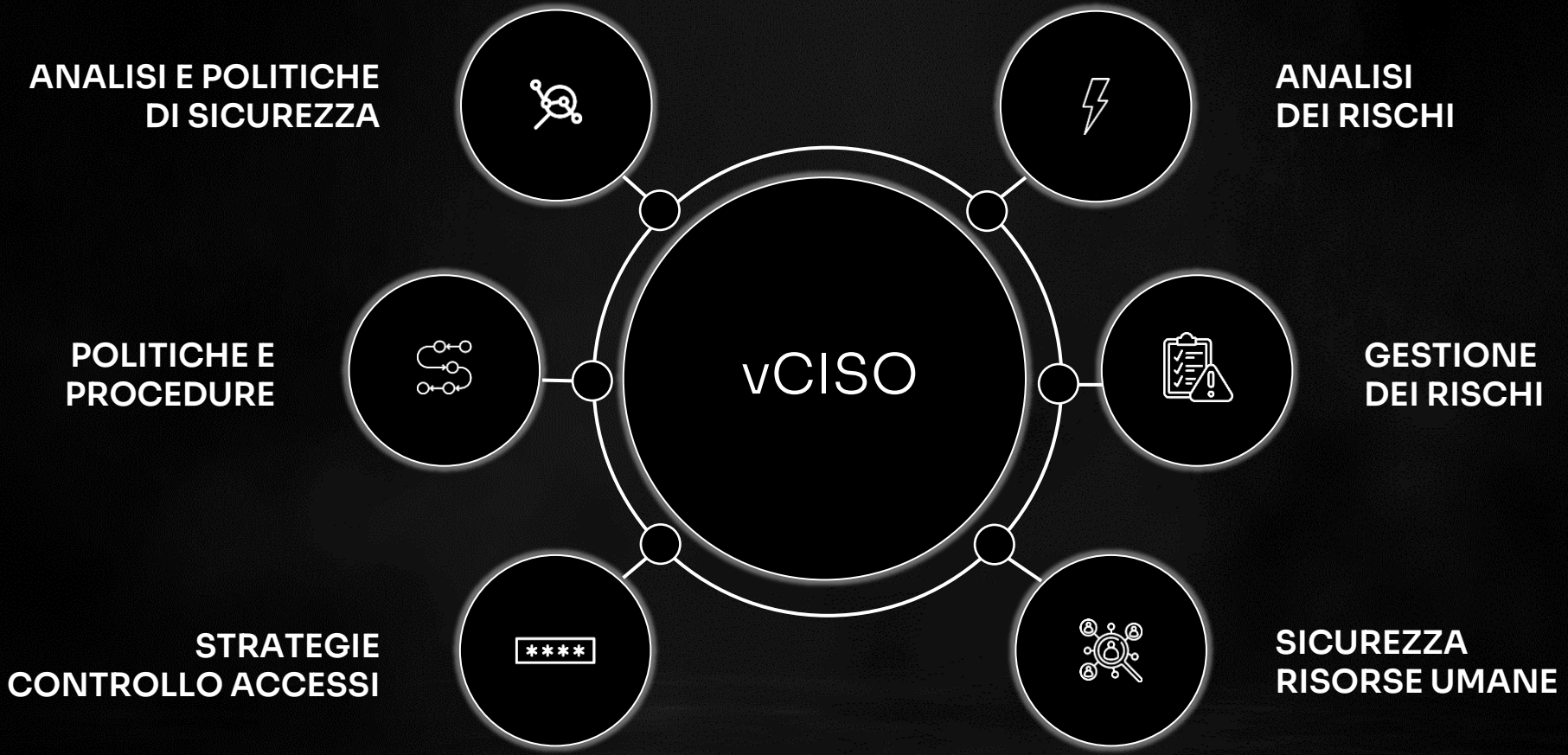
CYPEER E CSI PER NIS2



TITAAN NEEMESI PER NIS2



VIRTUAL CISO PER NIS2



Q&A

CONTACT US

Cyberoo S.p.A.
Via Brigata Reggio, 37
42124 Reggio Emilia

Tel. 0522.388111

Mail: info@cyberoo.com

Web: www.cyberoo.com

LinkedIn: CYBEROO

YouTube: CYBEROO

X: CYBEROO

Instagram:
@cyberoo_official