Cyber Risk Investigation

Conosci il rischio, proteggi il futuro.

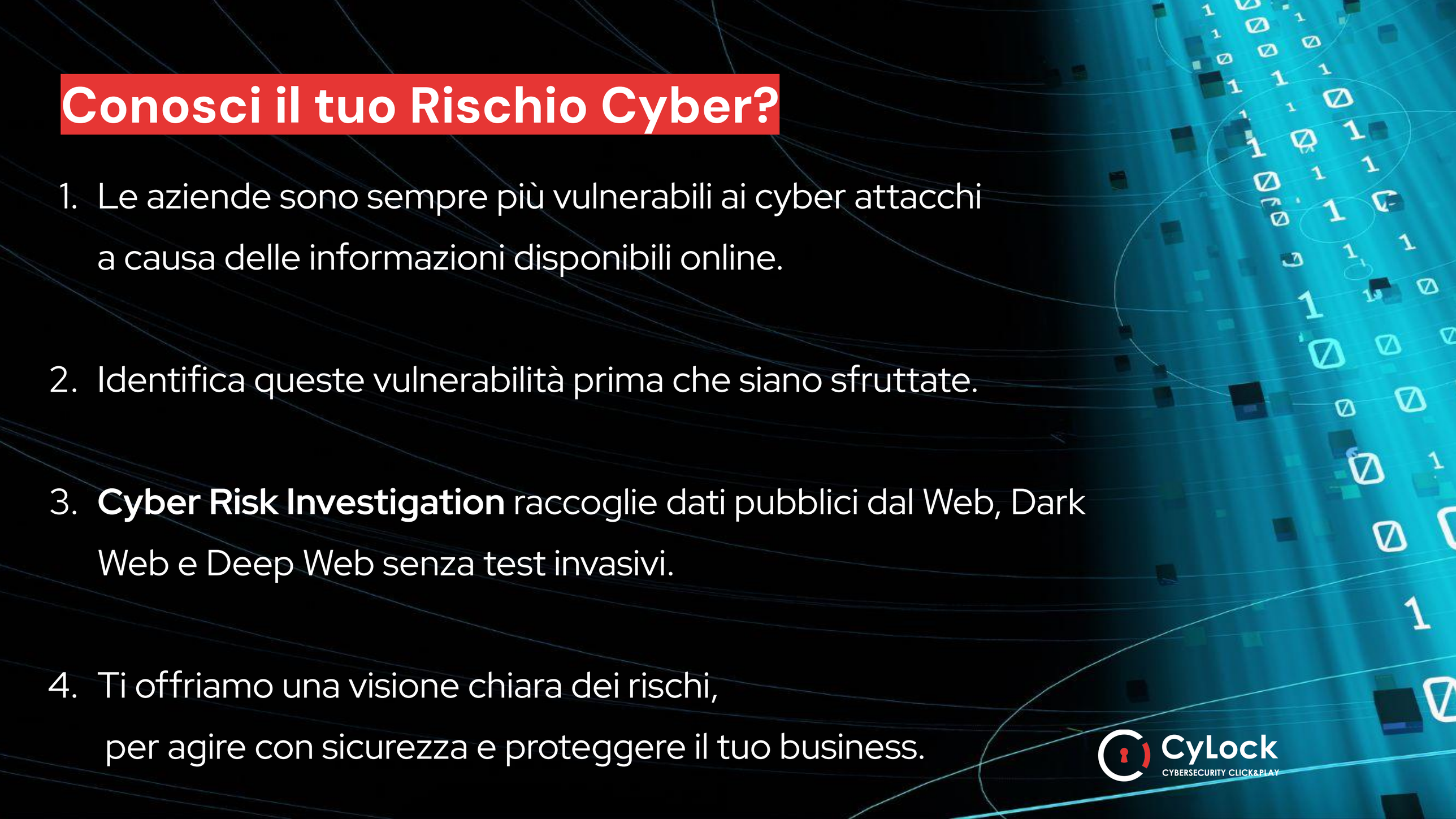
Conosci il tuo Rischio Cyber?

1. Le aziende sono sempre più vulnerabili ai cyber attacchi a causa delle informazioni disponibili online.

2. Identifica queste vulnerabilità prima che siano sfruttate.

3. **Cyber Risk Investigation** raccoglie dati pubblici dal Web, Dark Web e Deep Web senza test invasivi.

4. Ti offriamo una visione chiara dei rischi, per agire con sicurezza e proteggere il tuo business.



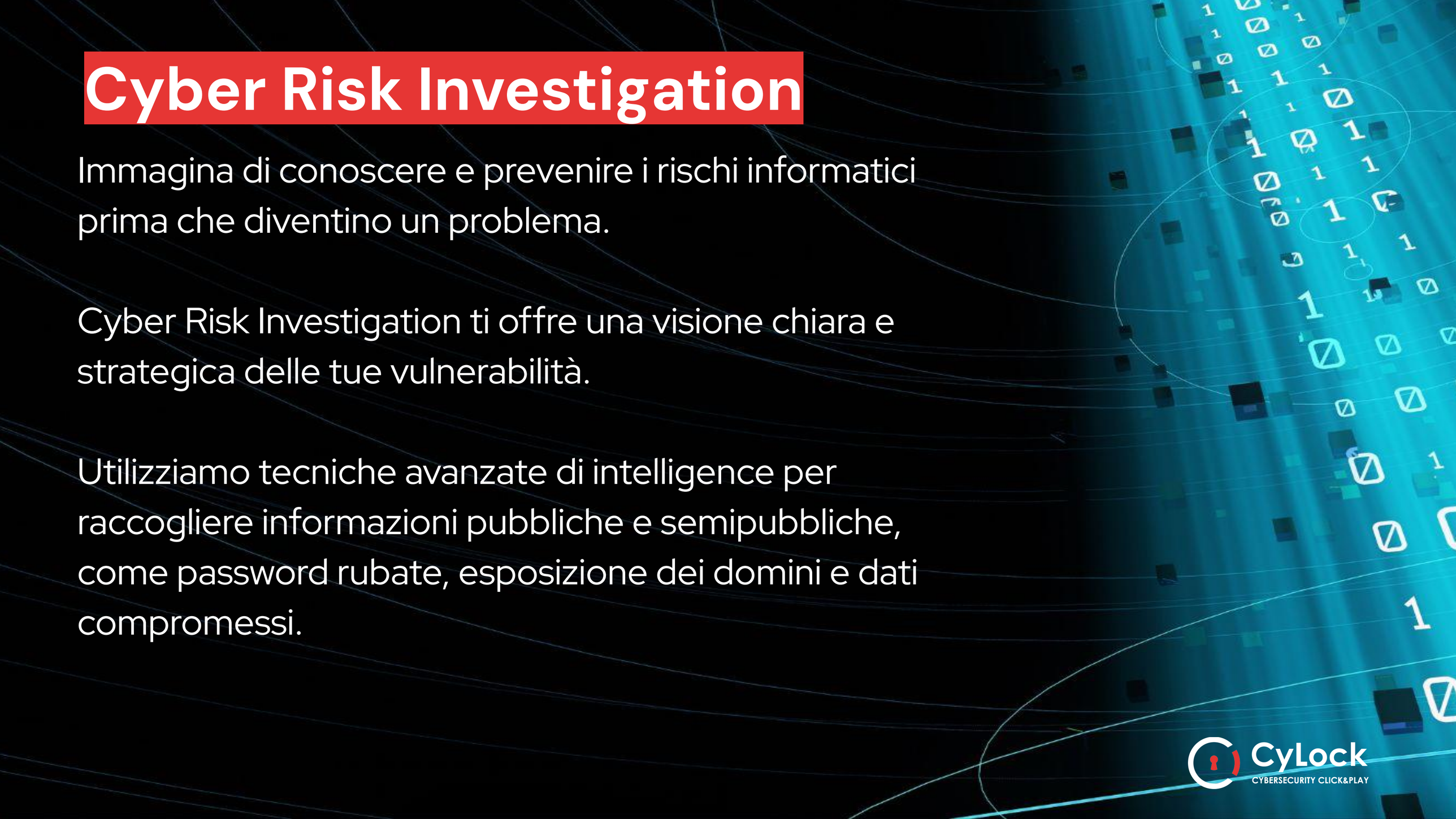
CyLock
CYBERSECURITY CLICK&PLAY

Cyber Risk Investigation

Immagina di conoscere e prevenire i rischi informatici prima che diventino un problema.

Cyber Risk Investigation ti offre una visione chiara e strategica delle tue vulnerabilità.

Utilizziamo tecniche avanzate di intelligence per raccogliere informazioni pubbliche e semipubbliche, come password rubate, esposizione dei domini e dati compromessi.



CyLock
CYBERSECURITY CLICK&PLAY

Indice di Rischio

Il Cyber Risk Index indica il livello di rischio di attacco aziendale in considerazione dei valori e dati raccolti e analizzati il suo andamento nel tempo, relativamente al dominio aziendale.

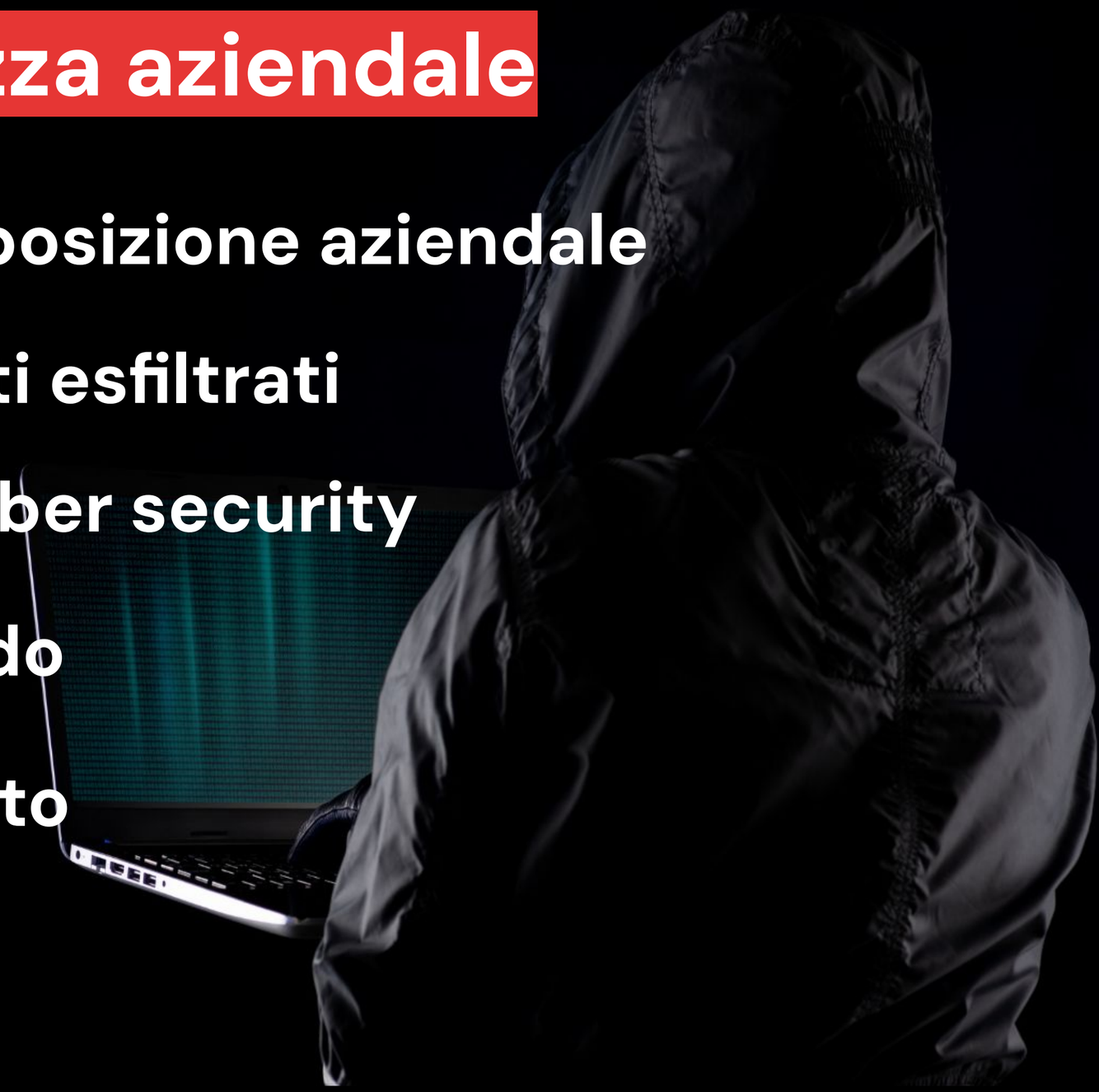
Tale indice si basa su:

- Analisi e data di rilascio dei data leak, quali email aziendali e password sottratte ai dipendenti;
- Analisi del numero di servizi esposti;
- Analisi delle informazioni pubbliche in mano agli Hacker.

CyLock
CYBERSECURITY CLICK&PLAY

Migliora la sicurezza aziendale

- Comprensione esposizione aziendale
- Identificazione dati esfiltrati
- Entry point per cyber security
- Accessibile e rapido
- Approccio Integrato con EVA



Cosa cerchiamo nel Dark Web?

- Credenziali mail e password
- Cookies
- Data base aziendali
- JSON Files
- Altro e informazioni

Quali informazioni troviamo con l’OSINT?

- URLs
- IPs
- Domini aziendali
- Typo domains e typo squatting
- E-mails

Cyber Risk Investigation

Cosa fare con le informazioni trovate

Credenziali nel darkweb

- **Cosa è successo**: Le credenziali sono state rubate/trovate
- **Rischi:**
  - Phishing: le mail possono essere usate per campagne mirate di Phishing. Campagne customizzate utilizzando anche dalle ulteriori informazioni rilasciate sui siti terzi (data di nascita, cellulari, indirizzi fisici)
  - Account Take Over: furto dell'identità, in particolare gli account social. In questo modo è possibile inviare messaggi con link malevoli ai propri contatti
  - Credential Stuffing: utilizzo delle credenziali per accedere ai servizi esposti su internet (VPN, webmail, gestionali)
- **Cosa fare:**
  - Cambio delle password e verifica delle policy di sicurezza
  - Anti-Phishing simulation e cybersecurity awareness – training
  - Review *endpoint protection* (antivirus/malware/firewall)

Cookies nel darkweb

- **Cosa è successo**: un PC è stato violato
- **Cause**: Attacco/Malware/Add-on browser
- **Cosa fare:**
  - Identificare il punto debole - Effettuare un test EVA
  - Proteggere i dispositivi - Review Policy/Tool di *endpoint protection* (antivirus/malware/firewall e tool gestione patch)
  - Proteggere la rete - Implementare soluzioni di IDS/DLP

Perimentro URL

- Rischio: Attacco Hacker
- Cause: Link a file sensibili esposti, errata configurazione del Server, phishing, condivisione accidentale, backup non protetti
- Cosa fare:
  - Testare il URL e server (EVA)
  - Verificare le informazioni (privacy)
  - Adottare una policy adeguata (IAM) e valutare un EDR
  - Promuovere la cybersecurity awareness – training

Rete IP pubblica

- Rischio: Attacco Hacker
- Cause: Configurazioni standard e dispositivi non monitorati
- Cosa fare:
  - Testare tutti gli IP di appartenenza (EVA)
  - Effettuare un assessment security (inventario registri e asset)
  - Verificare le policy di sicurezza
  - Valutare il sistema di firewall e l'xDR adottato/adottabile

Perimetro domini

- Rischio: Attacco Hacker
- Cause: Espansione digitale non controllata (policy), errori di configurazione, phishing
- Cosa fare:
  - Effettuare un assessment security (inventario asset, EVA)
  - Verificare le policy di sicurezza
  - Valutare strumenti per la gestione dei DNS, che offrono servizi CDN e protezione DDoS

Recap

- Le informazioni aziendali potrebbero essere già accessibili nel Dark Web.
- Questo aumenta il rischio di attacchi mirati e danni economici.
- Cyber Risk Investigation identifica queste esposizioni senza interventi diretti sui tuoi sistemi.
- La cybersecurity predittiva è la prima linea di difesa
- Cyber Risk Investigation ti dà le risposte per agire prima e prevenire gli attacchi informatici.

CyLock
CYBERSECURITY CLICK&PLAY