Cymulate

by

EXCLUSIVE NETWORKS

IT környezetek töréstesztje

SZABÓ Loránd & DÉVÉNYI Viktor
Exclusive Networks Hungary

Tesztelés és ellenőrzés fontossága más iparágakban?

Cymulate

EXCLUSIVE NETWORKS

Javasolt cél

Csökkenteni a sikeres támadás kockázatát,

a biztonsági környezet **ellenőrzésével** és behatolási módszerek **tesztelésével**.

Automatizáltan és folyamatosan, kulcsrakészen és testreszabhatóan.

Cymulate

Skálázható megoldás a kiberbiztonsági megfelelőség érdekében

CART | Continuous Automated Red Teaming: Célzott támadásokkal való automatizált tesztelés és támadási útvonal felderítés

BAS | Breach and Attack Simulation: A biztonsági környezetek rendszeres tesztelésére, mérésére és megfelelőségvizsgálatára való, kulcsrakész és állítható szimulációk

ASM | Attack Surface Management: Automatizált felderítés és priorizálás a külső- és belső támadási vetületek kitettségei számára

FELMÉRÉS | **OPTIMALIZÁLÁS** | **RACIONALIZÁLÁS** | **BIZONYÍTÁS**

Cymulate

EXCLUSIVE NETWORKS

FELMÉRÉS

Mérjük fel a biztonsági környezetünk és szabályozásaink jelenlegi állapotát

és hozzunk belőle létre fenntartható fejlődési irányt

Fedezzük fel

A kockázatokat Belső és Külső támadási felületeinken. Azonosítsuk az ismert és ismeretlen (ShadowIT) rendszereinket, tekintsük át a kitettségeket és priorizáljuk a kapcsolódó teendőket.

Validájuk

Az önálló és kombinált erősségeket és gyengeségeket a biztonsági szabályozásokban, szegmentálásban és stratégiánk más elemeiben.

Detektáljuk

A szabályozásokban jelenlévő gyenge pontokat, változtatásokat és azok hatását az infrastrukúránkra, fenyegetettségi látképünkre.

OPTIMALIZÁLÁS

Végezzünk finomhangolásokat, hogy eszközeink életciklusa optimális legyen

és tudjuk, ha új technológia beépítése szükséges

Találjuk meg a redundanciát

Ahol a rendszereink és kontroljaink átfedik egymást és hogy esetleg található-e ezt helyettesítő alternatíva

Rendszerek finomhangolása

Tartsuk a szabályokat és szabályozásunkat naprakészen, megfeleltetve jelenlegi és jövőbeni kihívásoknak

Folyamatok finomhangolása

Incidenskezelési (IR) és SOC műveleteink még hatékonyabbá tétele

Értékeljük ki az új kontrollokat

Hol nem lehetséges a réseket a jelenlegi folyamatokkal és technológiákkal kezelni; mutassunk rá és ellenőrizzük az új eszközök és folyamatok megfelelő létrejöttét

RACIONALIZÁLÁS

Elemzések, üzleti- és technikai riportok a ráfordítások optimalizálásához

és a megtérülés értelmezéséhez

Igazoljuk ráfordításainkat

A vezetőség számára, a budget megfelelő méretezése és célokhoz illő felhasználása

Kockázati értékelés, metodikák

Objektív, szabványokon alapuló riportokkal pozícionáljuk a szervezet biztonsági helyzetét. MITRE és NIST megfeleltetések.

Mutassuk fel az értéket

Validáljuk a jelenlegi eszközök, folyamatok, költések gyakorlati hasznait

Készüljünk fel

Azonosítsuk a harmadik fél által hordozott kockázatos metódusainkat

BIZONYÍTÁS

Megerősíteni, hogy az elhárítás a megfelelő hatást váltotta ki

és nem jött létre újabb gyengeség a folyamat során

Elhárítási folyamatok tesztelése

Szabályozásunk és biztonsági környezetünk változásai valóban megoldották a problémát és lezárták a rést? Teszteljük le.

Kerüljük el új rések kialakulását

Korrekciókkal új rések fennmaradását vagy akár létrejöttét előzhetjük meg, kezdve a gyorsan kivitelezhető, könnyen elháríthatókkal

Folyamatos vizsgálat

Hogy az idő haladtával, a változó környezeti elemek és üzleti folyamatok és a változó fenyegetettségi látkép által okozott hiányosságok feltárása megtörténjen

Cymulate

Skálázható megoldás a kiberbiztonsági megfelelőség érdekében

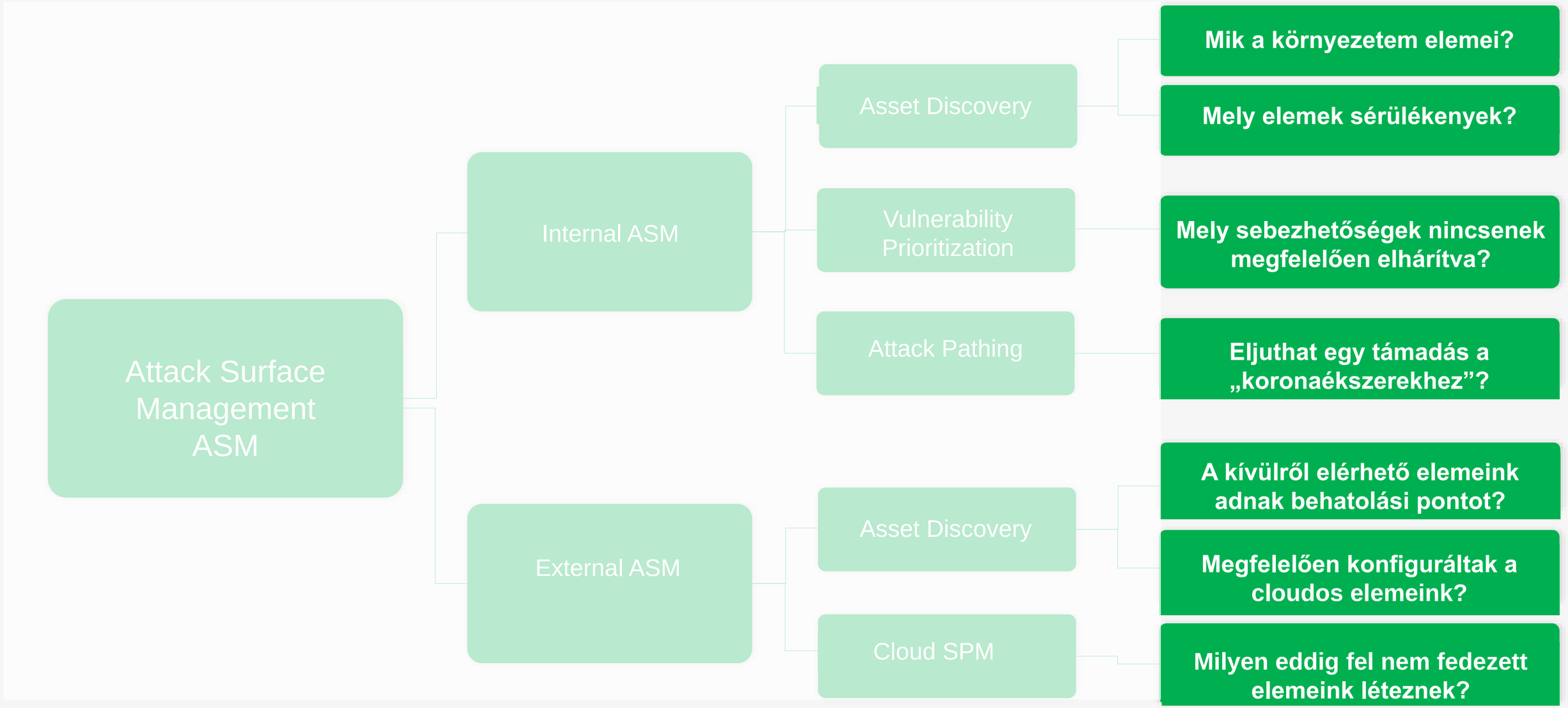
CART | Continuous Automated Red Teaming: Célzott támadásokkal való automatizált tesztelés és támadási útvonal felderítés

BAS | Breach and Attack Simulation: A biztonsági környezetek rendszeres tesztelésére, mérésére és megfelelőségvizsgálatára való, kulcsrakész és állítható szimulációk

ASM | Attack Surface Management: Automatizált felderítés és priorizálás a külső- és belső támadási vetületek kitettségei számára

FELMÉRÉS	OPTIMALIZÁLÁS	RACIONALIZÁLÁS	BIZONYÍTÁS

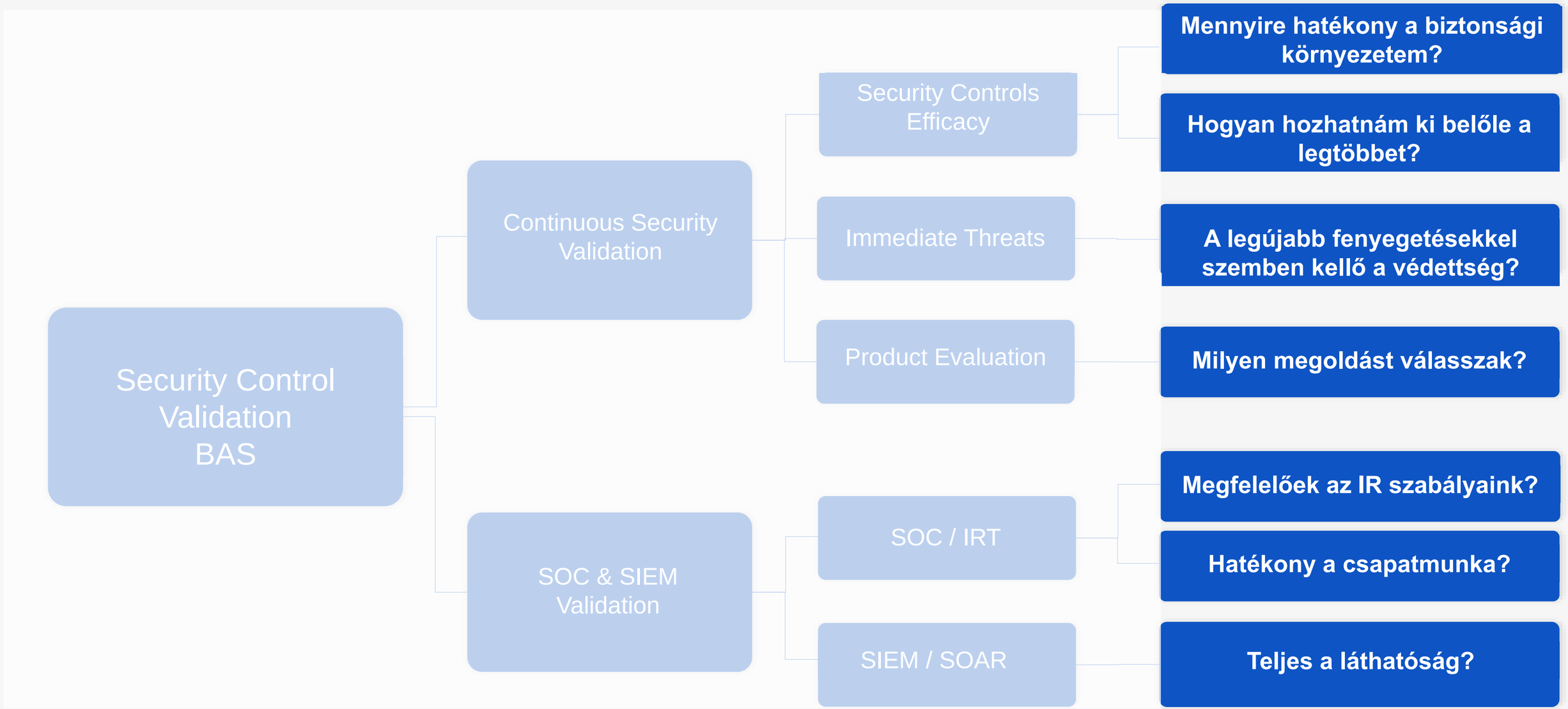
Attack Surface Management



Cymulate

EXCLUSIVE NETWORKS

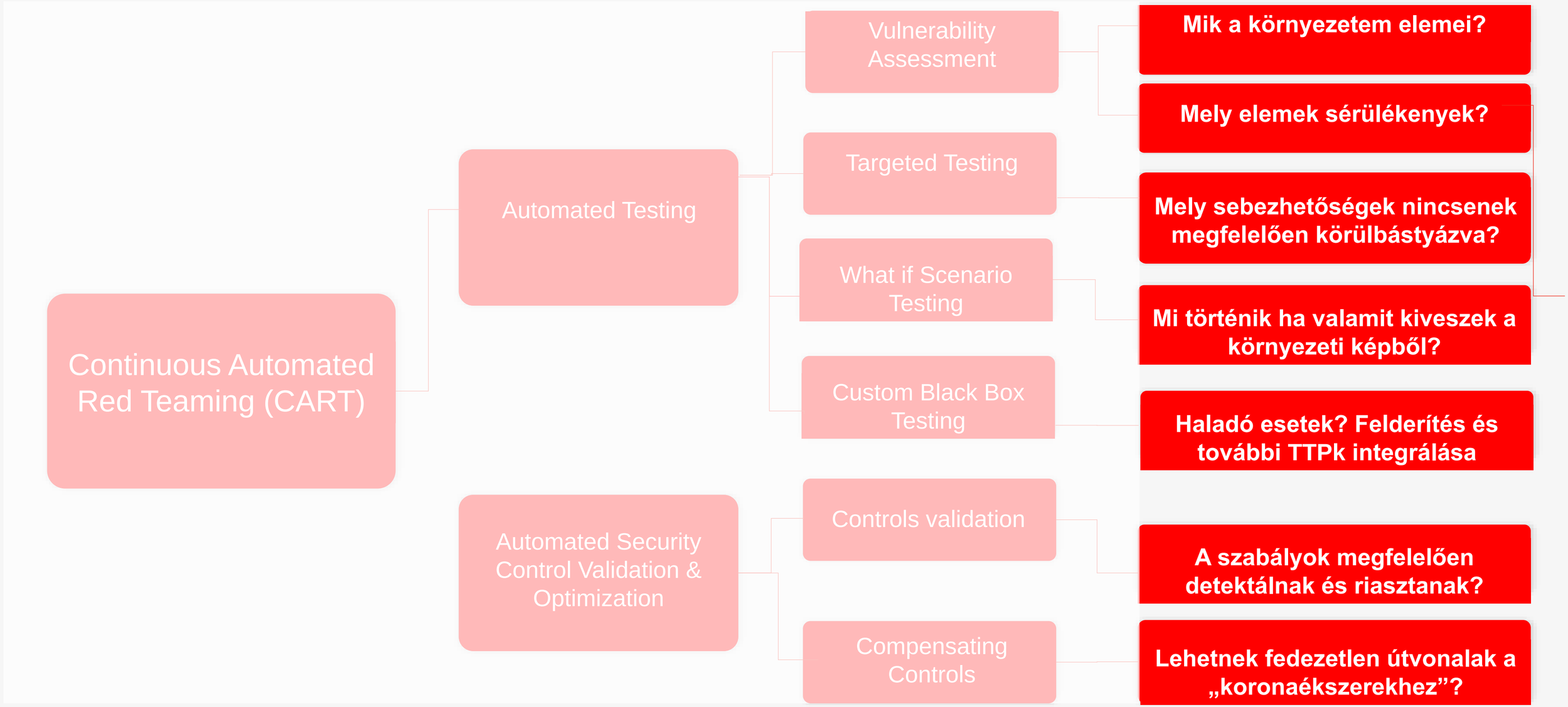
Breach and Attack Simulation



Cymulate

EXCLUSIVE NETWORKS

Continuous Automated Red-Teaming (CART)



Cymulate

EXCLUSIVE NETWORKS

Egy adatvezérelt, biztonsági szabályozásokat ellenőrző és kockázati kitettségelemző rendszer

Egyszerű telepítés és használat

- SaaS alapú, moduláris, akár egy óra alatt indítható
- Kulcsrakész vizsgálatok minden képességi szinthez

Átfogó lefedettség

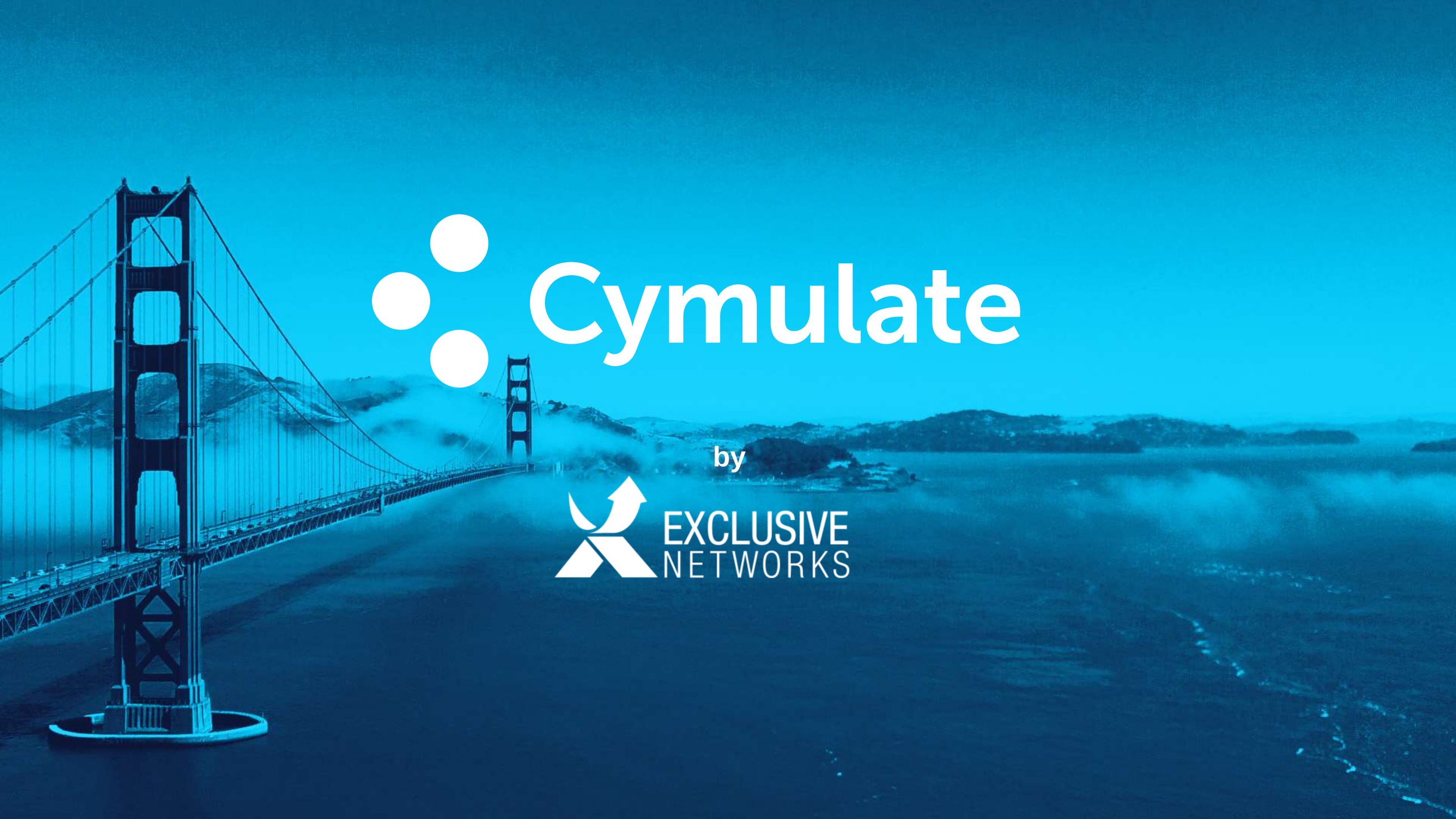
- Az APT támadások teljes támadási láncolatát lefedi, láthatóvá és kezelhetővé teszi
- Vektoronkénti, részletes megfeleltetés és optimalizálás

Nagyfokú állíthatóság

- Red/Purple Teaming automatizálása, a támadói csoportok fejlettsége szerint
- A saját környezetünkhöz illeszthető, automatizált ellenőrzések

Cymulate

EXCLUSIVE NETWORKS


Cymulate
by
EXCLUSIVE
NETWORKS