HAGYJUNK FEL A SÉRÜLÉKENYSÉGEK VADÁSZATÁNAK ROSSZ GYAKORLATÁVAL!

Bemutatkozik a fenyegetettségközpontú sérülékenység menedzsment

SKYBOX™ SECURITY

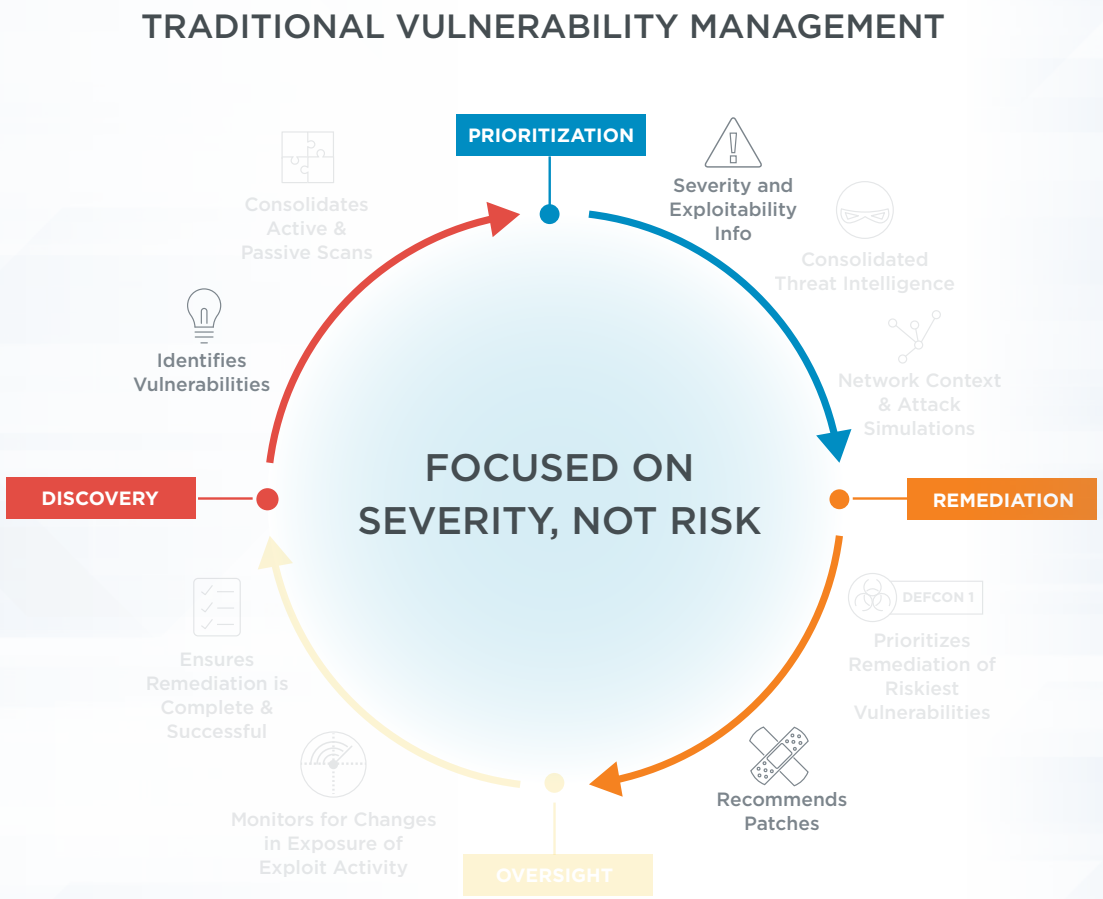
Total Visibility. Focused Protection.™

A probléma

A sérülékenységek kezelése és az azokkal kapcsolatban felmerülő kockázatok csökkentése a biztonsági szoftverek alapvető feladata, ennek ellenére a védekezés során sokszor kritikus fontosságú lépéseket hagynak figyelmen kívül. Így például gyakran szorul háttérbe a biztonsági hibák priorizálása. Megfelelő adatok és a kontextusok felállítása nélkül pedig nem lehet hatákonyan csökkenteni a kockázatokat, és rugalmasan reagálni a felmerülő veszélyekre.

A hagyományos megközelítés hátrányai

- ☒ Az aktív szkennerek a sérülékenységek felkutatása közben problémákba ütközhetnek a nem ellenőrizhető hálózati eszközök és zónák miatt.
- ☒ A vállalati hálózatok ellenőrzése sok időt emészthet fel, miközben a védelmi adatok elavulttá válnak az idő múlásával.
- ☒ A hagyományos védelmi eszközök nem ismerik a hálózati topológiát és a biztonsági kontrollokat, ami negatív hatással lehet a sérülékenységek kezelésére.
- ☒ A kevesebb kockázatot hordozó hibák kezelése sok időt rabolhat el, miközben a valóban súlyos sérülékenységek elhárítására nem marad elegendő erőforrás.



Miközben a sérülékenységek felderítését végző szkennerek elengedhetetlen összetevői a sérülékenység menedzsment rendszereknek, addig ezek gyakorta nem alkalmazzák vagy nem veszik figyelembe a kontextus alapú elemzéseket, amik révén meghatározható lenne, hogy mely biztonsági rést kell először befoltozni. Ha pedig több gyártó szkennere működik párhuzamosan, akkor az több erőforrást igényel az adatok központosított kezeléséhez és összefésüléséhez, illetve a sérülékenységi elemzések konzisztenciájának fenntartásához.

Hatékony megoldás a sérülékenység menedzsmentre

A fenyegetettségközpontú sérülékenység menedzsment, TCVM (Threat Centric Vulnerability Management) egy alapjaiban új megközelítés a szervezeteket érő támadások jelentette kockázat jelentős mértékű csökkentésére. Kontextus alapú technikát alkalmaz a hálózat, az üzleti folyamatok, a digitális adatvagyon, valamint a fenyegetettségi térkép vonatkozásában.

A TCVM előnyei

- Csökkenti a támadások sikerességének valószínűségét azáltal, hogy azokra a sérülékenységekre fókuszál, amelyek a legnagyobb valószínűséggel kapnak szerepet az incidensekben.
- Csökkenti a felesleges patch-elések számát, és a leghatékonyabb kockázatcsökkentő lehetőségeket kínálja.
- A hálózati, az üzleti és a digitális adatvagyon, valamint a patch menedzsment adatokat egy egyszerű felületen keresztül teszi kezelhetővé az éppen aktuális fenyegetettségi térkép alapján.
- Automatizálhatóvá teszi a sérülékenységek kezelésével összefüggő feladatokat.

A veszélyesség nem egyenlő a kockázattal

A hagyományos sérülékenység menedzsment a biztonsági hibák veszélyességi besorolásából indul ki. Ez azonban nem elégséges a valódi kockázatok megértéséhez.

A veszélyességi besorolásokra való összpontosítás önmagában nem hatékony, ettől ugyanis még sérülékeny maradhat a szervezet. Ezért teljes körű, összefüggés alapú elemzésekre van szükség.

1. eset

Azon kritikus sérülékenységek kezelése felesleges, amelyeket más biztonsági kontrollok kiküszöbölnek.

2. eset

Azon alacsonyabb veszélyességű, javítatlan hibák, amik aktív szerepet kapnak támadásokban, komolyan kockáztatják a hálózat épségét.

100%-os

NÖVEKEDÉS A CVE-BESOROLÁSÚ SÉRÜLÉKENYSÉGEK SZÁMÁBAN*

Hova kell összpontosítani az erőforrásokat?

60%-os

NÖVEKEDÉS AZ ÚJ EXPLOITOK HAVI SZÁMÁBAN**

Hogyan maradjunk egy lépéssel a támadók előtt?

76%-a

AZ EXPLOITOKNAK SZERVER OLDALI ALKALMAZÁST SÚJT**

Hogyan ismerjük fel a veszélyeket?

120%-os

NÖVEKEDÉS AZ OT SÉRÜLÉKENYSÉGEKBEN**

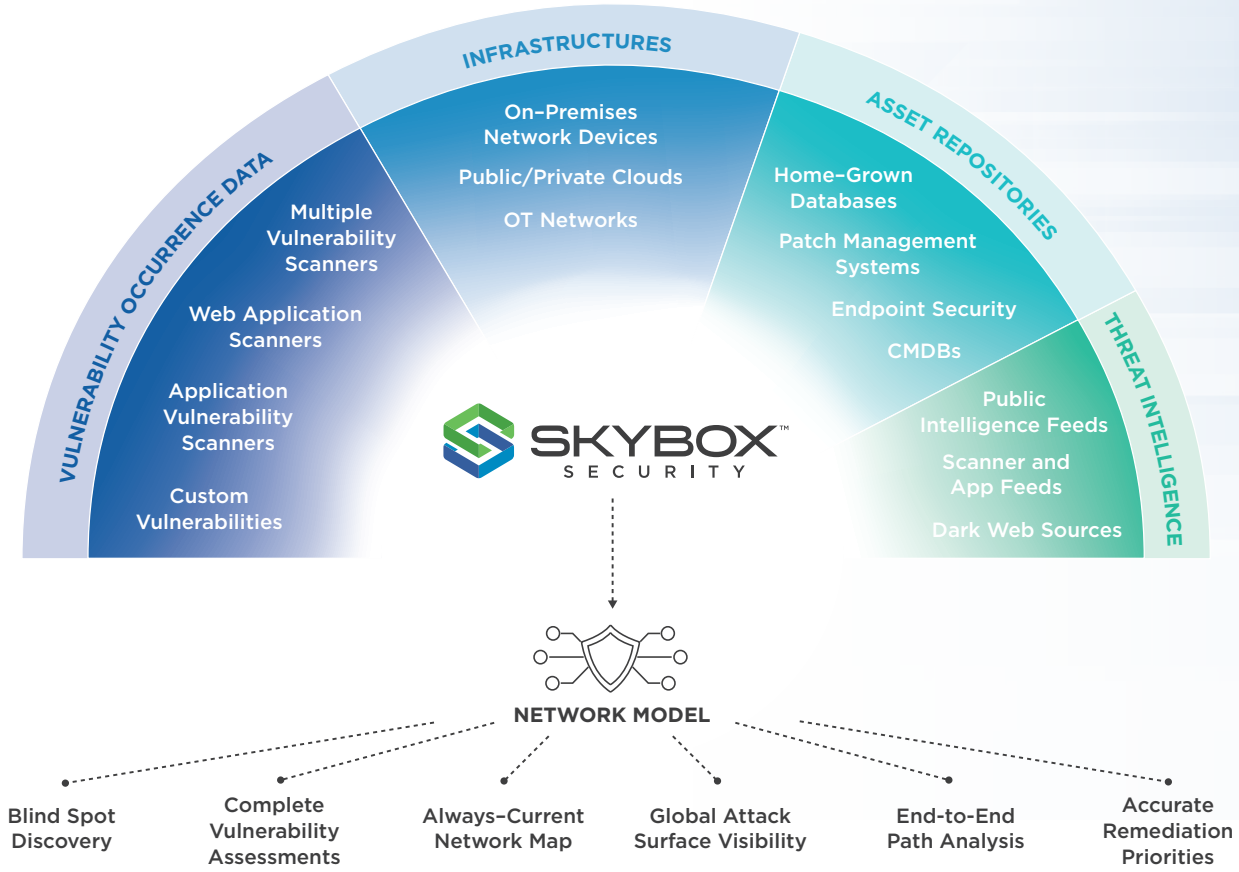
Hogyan kezeljük a nem ellenőrizhető zónákat, amikor az erőforrásaink korlátozottak?

* "CVSS Severity Distribution Over Time," National Institute of Standards and Technology, January 12, 2018. https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

** "Vulnerability and Threat Trends Report 2018," Skybox Security, February 6, 2018. https://lp.skyboxsecurity.com/WICD-2018-02-Report-Vulnerability-Threat-18_Asset.html.

Több tartalom, mélyebb összefüggések

A Skybox olyan módon kezeli a sérülékenységeket, mintha azok egy nagyobb támadási felület részei lennének. Számos adatforrásból - beleértve a hálózatot és a védelmi alkalmazásokat is - gyűjti az adatokat, hogy azok révén valóban megérhetők legyenek a kockázatok.



A sérülékenység menedzsment és a kockázat-csökkentés

A Skybox™ Security Threat–Centric Vulnerability Management (TCVM) egy okosabb, innovatívabb megközelítést alkalmaz a támadások kivédésének érdekében. Teljes mértékben kontextus alapú eljárásokra épül a támadási felületek tekintetében, és ilyen módon segíti a feladatok priorizálását.

A TCVM révén egy átfogó, pontos kép rajzolódik ki az adott IT-környezet sérülékenységeiről. A kockázatokat összekapcsolja a sérülékenységekre való reagálással, amivel nagymértékben csökkenti a támadások sikerességének valószínűségét.

A TCVM FOLYAMAT NÉGY LÉPÉSE

1. LÉPÉS
FELDERÍTÉS

A sikeres sérülékenység menedzsment a pontos sérülékenységi adatok megléténél kezdődik. Az aktív szkennelés egy fontos lépése a felderítési fázisnak, de vannak korlátai.

Hagyományos szkenner technológiák már 30 éve léteznek, de napjaink hálózatai sok mindenben különböznek a 90-es évek hálózataitól.

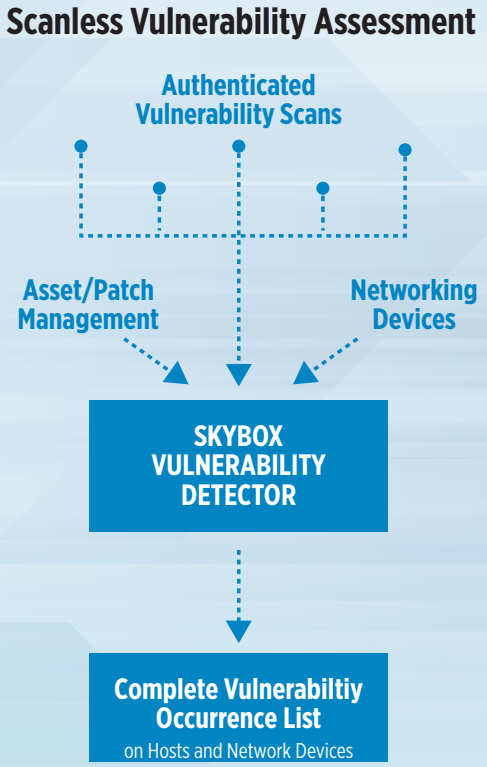
- **Szkennelés a felhőben:** a felhős hálóztatok folyamatosan változnak, az erőforrások offline állapotba kerülhetnek, és módosulhatnak az utolsó ellenőrzés óta. Ráadásul sok szervezet több szolgáltatóval is együttműködik.
- **Szkennelés az OT hálózatokban:** az OT hálózatok korlátozhatják az aktív szkennelést, és nem megfelelően patch-elt eszközök maradhatnak a hálózatban.

Ezért szükség van passzív megoldásokra, hogy a dinamikus környezetekben lévő vakfoltok felfedhetővé váljanak.

A Skybox™ Vulnerability Detector passzív, szkennelés nélküli sérülékenység menedzsmentet biztosít, amely igény szerint futtatható, és a teljes hálózatot percek alatt feltérképezi. A Skybox megfelelteti a Vulnerability Detectorból származó eredményeket más gyártók megoldásaival annak érdekében, hogy központosítsa a sérülékenységi adatokat, valamint erős alapot képezzen a további TCVM folyamatok számára.

Skybox megközelítés

- A patch- és eszközmenedzsment rendszerek, valamint a konfigurációs naplók alapján 99 százalékos pontosságú sérülékenység felderítés
- Passzív sérülékenység detektálás dinamikus, multi-cloud környezetekben
- Információk normalizálása és összehasonlítása a Skybox biztonsági intelligenciájával
- Perceken belül elérhetővé váló sérülékenységi információk
- Az aktív szkennerek által hagyott vakfoltok feltárása



FELDERÍTÉS

Az eszköz, a sérülékenységi és a hálózati adatok összesítése

A TCVM sarokköve, hogy az infrastruktúra pontosan feltérképezhető legyen. Ehhez elengedhetetlen, hogy megértsük a védelmi ellenőrzés működését azokon a pontokon, ahol kritikus adatok kezelése történik, és amelyek potenciális támadási felületekhez kapcsolódnak.

Miközben az aktív szkennerek által gyűjtött adatok hasznosak a sérülékenységek feltárásához, mégsem képesek teljes körű adatgyűjtésre a kockázatok kimutatásához, a priorizáláshoz és a kockázatcsökkentéshez.

- **Hiányos, decentralizált adatok:** sok szervezet használ különféle szkennereket és egyéb védelmi megoldásokat a biztonsági gyengeségek felderítéséhez. Azonban egyik szkenner sem képes központosított információkezelésre. Tipikusan ezeknek nem feladata az adatok importálása és összegzése.
- **Kontextus nélkül:** a hagyományos szkennerek általában nem veszik figyelembe a hálózatbiztonsági eszközök által biztosított lehetőségeket. Enélkül pedig különböző erőforrásokat hagyhatnak védtelenül. Továbbá nem képesek a patch-elésen kívül további védelmi ajánlások megtételére.

A Skybox Security egyedülállóan gyártó-tudatos a tekintetben, hogy képes különböző adatforrásokból importálni és központosítottan elérhetővé tenni adatokat, beleértve a hálózatbiztonsági eszközöket, a biztonsági intelligencia megoldásokat és a sérülékenységi adatbázisokat is. Ezek kombinálása a szkennelés nélküli technológiákkal biztosítja azt, hogy a sérülékenységek feltárása pontos legyen, és a teljes IT-környezetre kiterjedjen. Ezzel kiváló alap teremthető az egész TCVM workflow számára.

A Gartner 10 sérülékenységi faktora

1. Veszélyesség
2. Megfelelőség
3. Kor
4. Hely
5. Kihasználhatóság
6. Előfordulás
7. Szerepkörök
8. Eszközök
9. Fenyegetettségek
10. Hálózati topológia

Megfelelő eszközmenedzsment és hálózat nélkül lehetetlen minden tényezőt kezelni.

Forrás: "A Guidance Framework for Developing and Implementing Vulnerability Management," Gartner, June 22, 2017. https://www.gartner.com/doc/3747620/guidance-framework-developing-implementing-vulnerability

2. LÉPÉS
PRIORIZÁLÁS

A LEGNAGYOBB KÜLÖNBSÉGET

a hagyományos megközelítések és a TCVM között azok az elemzések jelentik, amelyek lehetővé teszik a priorizálást. A Skybox a sérülékenységek kockázatának értékelése során nem csak a sérülékenységek veszélyességére koncentrál, hanem több tényezőt vesz figyelembe.

IDENTIFY KNOWN VULNERABILITIES

Total identified vulnerabilities via Skybox intelligence feed

IDENTIFY YOUR VULNERABILITIES

Third-party scanners and Skybox Vulnerability Detector

PINPOINT BIGGEST RISKS

Skybox Vulnerability Control Prioritization Center

IMMINENT THREATS (HIGHEST PRIORITY)

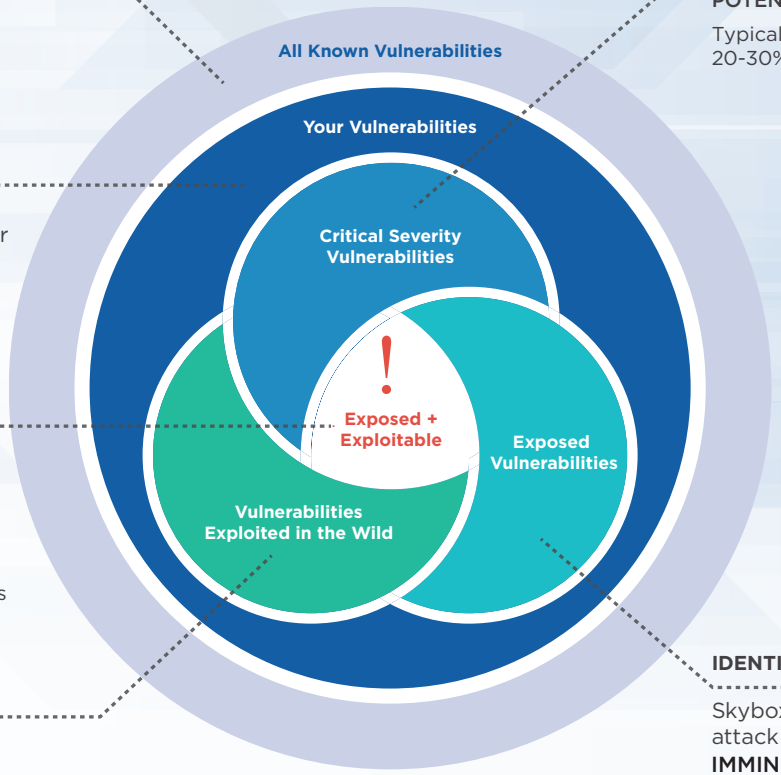
Typically account for <1% of vulnerability occurrences

IDENTIFY EXPLOITS

Skybox Research Lab threat intelligence

IMMINENT THREATS

Typically account for



CORRELATE TO CVSS

CVSS critical score

POTENTIAL OR IMMINENT THREATS

Typically account for 20-30% of vulnerability occurrences

IDENTIFY EXPOSURES

Skybox network modeling and attack vector analytics

IMMINENT THREATS

Typically account for 1% of vulnerability occurrences

PRIORIZÁLÁS

1 Sérülékenység

2 Sérülékenység felderítés

3 Fenyegetettség elemzés

4 Hálózat-felderítés

5 Elemzés és támadás-szimuláció

1. Meglévő sérülékenységek

A Skybox TCVM a szervezet jelenlegi sérülékenységeinek feltárásával veszi kezdetét.

2. Sérülékenységek felderítése

A Skybox biztonsági intelligenciát használ a sérülékenységek hatásainak minél pontosabb felméréséhez. Ennek alapjául olyan sérülékenységi adatbázisok szolgálnak, amik az ismert biztonsági rések pontos technikai jellemzőit foglalják magukban:

- Azon paraméterek, amelyek egy sérülékenység kihasználhatóságát befolyásolják (operációs rendszer, telepített alkalmazások stb.).
- A bizalmasságot, az integritást és az elérhetőséget befolyásoló tényezők.
- Sérülékenységek kutatása, National Vulnerability Database (NVD) listázás, gyártói közlemények stb.
- Hibajavítási és kockázatcsökkentési megoldások.
- Veszélyességi besorolások beszerzése több forrásból (NVD, IBM X–Force stb.) és Common Vulnerability Scoring System (CVSS) kategorizálás
- Sérülékenységi információk változáskövetése (veszélyesség, kihasználhatóság, elérhető patch-ek stb.)

3. Fenyegetettségek elemzése

A Skybox az exploitokról is gyűjt információkat. Például arról is, hogy melyek kerültek bele különféle malware-ekbe. A Skybox folyamatosan elemez nyilvános és privát adatforrásokat is a Skybox™ Research Lab segítségével. A védelmi információkhoz a Skybox termékek a Skybox intelligence feed technológia révén jutnak hozzá.

Biztonsági elemzések – ellenőrzött információk

A Skybox kutatói több tucat biztonsági adatforrást fésülnek át minden egyes nap. Figyelik az internet sötét oldalán működő weboldalakat, ellenőrzik, értékelik a fenyegetettségi térképet. A sérülékenységek kihasználására, veszélyességére, hatására vonatkozó információkat adnak ki. Támadási mintákat dolgoznak ki, amelyek alapján a szimulált támadások lefolytathatók. Ez a fajta biztonsági intelligencia nemcsak a TCVM folyamat részét képezi, hanem a Skybox™ Security Suite fontos alkotóeleme is.

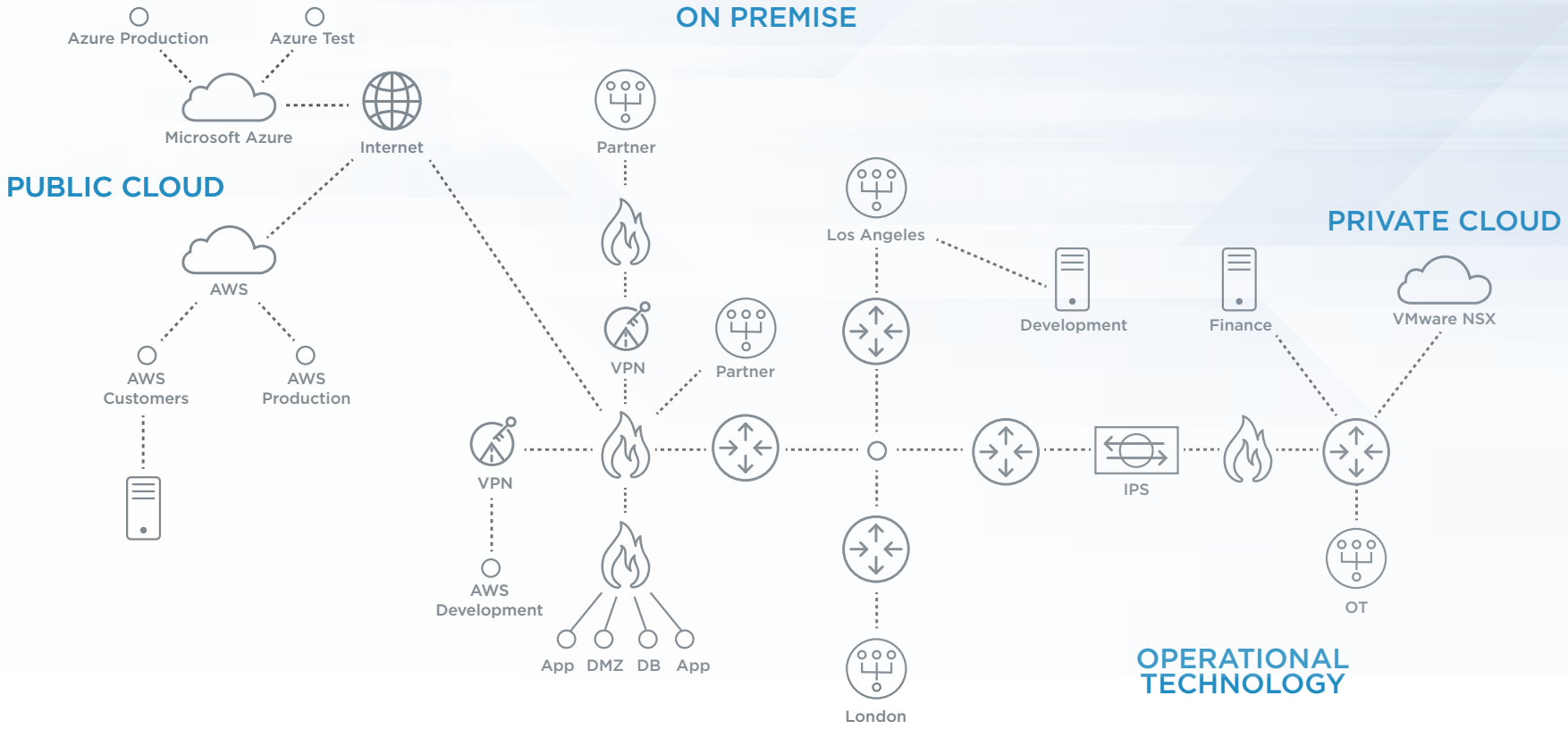
PRIORIZÁLÁS

4. Hálózatfelderítés

A Skybox elemzi a szervezet eszközeit, hálózatait és azok üzleti folyamatokra gyakorolt hatásait annak érdekében, hogy a támadási felületeket kimutathatóvá tegye. A támadási felületek alapján az IT-környezet paramétereinek figyelembevételével átfogó modelleket épít fel:

- Hálózati topológia (routerek, terheléselosztók, switch-ek)
- Biztonsági kontrollok (tűzfalak, IPS, VPN)
- Eszközök (kiszolgálók, munkaállomások, hálózatok — beleértve a hagyományos IT, a felhő alapú és az OT környezeteket)

A modell rendszeresen és automatikusan frissül a hálózat aktuális állapotának megfelelően.

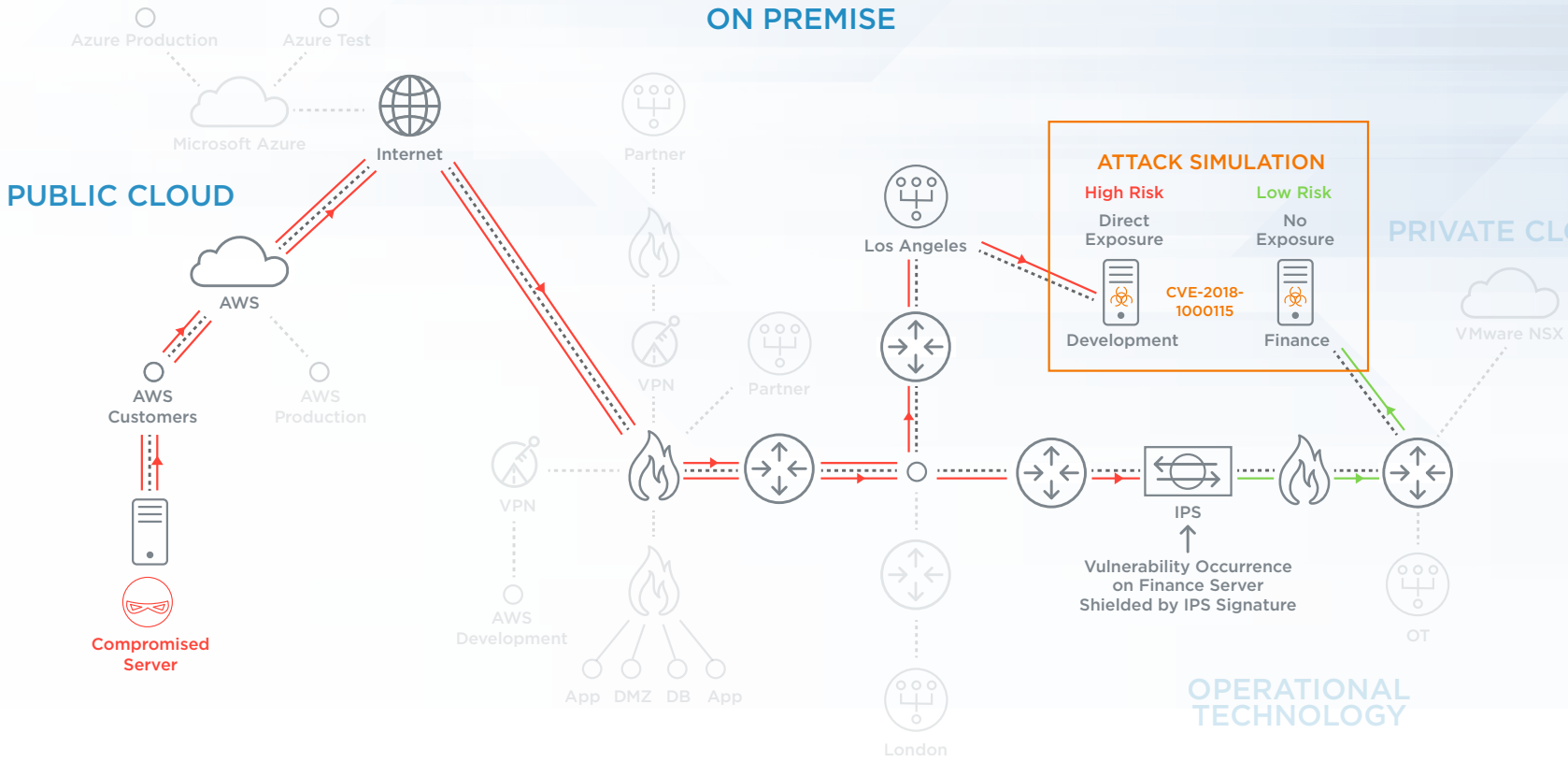


PRIORIZÁLÁS

5. Elemzés és támadásszimuláció

A sérülékenység elemzés a legkritikusabb lépés a hálózat különféle veszélyekkel szembeni kitettségének felmérése során. Ennek megértésével az erőforrások a veszélyes sérülékenységek kezeléséhez rendelhetők a támadási felületek csökkentése érdekében.

A Skybox a sérülékenységek kihasználhatóságát szimulált támadásokkal állapítja meg. Az automatizált szimulációk a fenyegetettségek belépési pontjától indulnak, és minden eszközhozzáférési forgatókönyvet számításba vesznek. Ezáltal kimutathatóvá válhat, hogy egy sérülékeny eszköz elérhető-e a támadók számára. Amennyiben igen, akkor a sérülékenység közvetlenül kihasználhatóvá válhat, és a Skybox futtat egy második elemzést is. Ekkor a sérülékeny eszköz már egy kompromittált erőforrásként jelenik meg, és több lépéses támadások szimulálására kerül sor (közvetett kihasználhatóság).



3. LÉPÉS
REAGÁLÁS

A TCVM priorizálás eredménye meghatározza a reagálás, hibajavítás folyamatát. A sérülékenységek öt veszélyességi kategóriába sorolhatók, amelyek mindegyike egyben kockázati szintet is jelent a javítások sürgősségének definiálásához.

A TCVM workflow első két lépésének (felderítés, priorizálás) köszönhetően az azonnali intézkedést igénylő (már kihasználás alatt álló) sérülékenységek száma kezelhetővé válik.

A legjobb kockázatcsökkentő lehetőségek

A Skybox TCVM megközelítése a sérülékenységek jellemzői, az IT-környezet és a támadási formák figyelembevételével több lehetőséget kínál a sérülékenységek kezelésére. Olyanokat, amelyek költséghatékonyan elvégezhetők, a lehető legkisebb kockázatot jelentik az üzletmenet folytonosságára, és hatékonyabb megoldást kínálnak, mint a hagyományos értelemben vett patch-elés.

SZIGNATÚRÁK:
Meglévő védelmi technológiák (IPS-szignatúrák, végpontvédelem) alkalmazása.

TŰZFAL:
A hoszt alapú tűzfalakon alkalmazandó szabályok beállítása a sérülékeny eszköz hozzáférhetőségének korlátozásához.

KONFIGURÁLÁS:
A sérülékeny szoftver átkonfigurálása a biztonsági rés kihasználásának megakadályozása érdekében.

FRISSÍTÉS:
Régi verzióról történő frissítés a sérülékenység javítása érdekében.

PATCH-EK:
Patch-ek telepítése az elérhető riasztások és javítások szerint.

A Skybox segítségével az IT munkatársak teljes körű rálátást kapnak a sérülékenységekre való reagálási lehetőségekre, és azok közül a legoptimálisabbat választhatják ki.

Reagálás OT hálózatokban

Az OT hálózatokban nem tolerálhatóak a leállások, így ezek a szervezetek gyakran halogatják a sérülékeny szoftverek frissítését. Amitől tartanak:

- Szolgáltatások elérhetetlenné válásától
- Rendszerekben bekövetkező károktól, sérülésektől
- Alkalmazottak, ügyfelek, közösségek veszélyeztetésétől
- Garanciavesztéstől

A Skybox TCVM megoldása képes kockázatcsökkentő alternatívákat kínálni a patch-elésre. Emellett priorizálással segíti a patch-elés koordinálását a hálózat tervezett leállítása során.

4. LÉPÉS
FELÜGYELET

A hálózatban előforduló sok eszköz és potenciális sérülékenység miatt könnyen előfordulhat, hogy átsiklunk egyébként fontos információkon. Ennek kockázatát a Skybox jelentősen csökkenti.

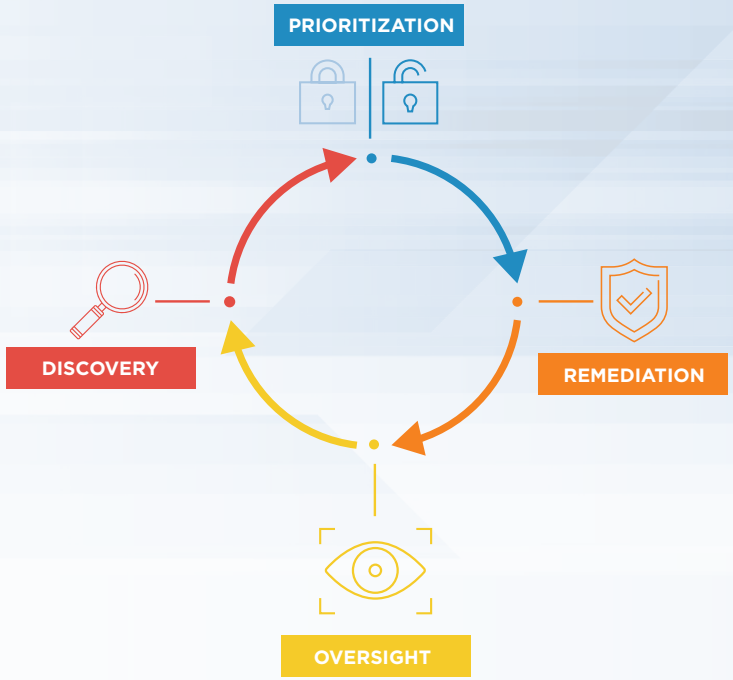
MONITOROZÁS:
A hálózat fenyegetésekkel szembeni kitettségének változása monitorozásra kerül az azonnali beavatkozások érdekében.

NYOMON KÖVETÉS:
A kockázatok nyomon követése biztosítja a fenyegetések gyors és teljes körű hatástalanítását.

KIMUTATÁSOK:
A trendek időbeli változásának figyelésével összehasonlíthatóvá válnak a múltbeli és a jelenlegi sérülékenységek kockázatai.

A felügyelet segíti az elszámoltathatóságot, a nyomon követést és annak biztosítását, hogy a reagálás, hibajavítás valóban hatékony és pontos legyen. Ahhoz, hogy biztosak legyünk egy sérülékenység maradéktalan megszüntetésében, a felügyeleti fázist be kell illeszteni a TCVM-be.

CONTINUOUS RISK REDUCTION WITH TCVM WORKFLOW



KOCKÁZATKEZELÉS TCVM ALAPOKON

Kizárólag a Skybox egyesíti azokat a technológiákat, amelyek segítségével lehetővé válik a fenyegetettségközpontú sérülékenység menedzsment, beleértve az adatgyűjtés és normalizálás automatizálását, a sérülékenységek támadási felülettel összefüggő priorizálását, a helyreállítási útmutatást és a felügyeletet.

A Skybox használatával a szervezet képessé válik:

AZ ERŐFORRÁSOKRA VALÓ KONCENTRÁLÁSRA

a sérülékenységek azon halmaza nagyobb valószínűséggel jut szerephez a szervezet elleni támadásokban, amelyeket egyébként is aktívan használnak ki a kiberbűnözők.

GYORSABB ÉS HATÉKONYABB REAGÁLÁSRA

a Skybox biztonsági intelligenciájának köszönhetően, valamint a hibajavítási útmutatók használatával.

IDŐ ÉS ERŐFORRÁS MEGTAKARÍTÁSRA

a sérülékenység menedzsmenthez kötődő feladatok automatizálásával.

A TELJES FOLYAMAT KEZELÉSÉRE

a sérülékenység menedzsment központosított megvalósításával.

AZ ÖSSZEFÜGGÉSEK MEGÉRTÉSÉRE

a hálózatban — legyen szó hagyományos, felhős vagy OT környezetről.

Következő lépések

TOVÁBBI INFORMÁCIÓK

https://www.skyboxsecurity.com/tcvm

PRÓBÁLJA KI

Demó:
https://lp.skyboxsecurity.com/WEB-Contact-Us.html

Skybox Security

A Skybox Security a kiberbiztonsági megoldások egyik vezető gyártója. Olyan integrált platformot biztosít, amely fejlett analitikával, automatizációval és biztonsági intelligenciával segíti a szervezeteket a védelem megerősítése és a mindenre kiterjedő kockázatcsökkentés területén. Folyamatosan erősíti pozícióját a nagy, komplex hálózatok világában, beleértve a hagyományos IT-t, a multi-cloud és az OT környezeteket. 120 hálózati és biztonsági technológia integrálásával a Skybox™ Security Suite kontextus alapú megközelítéssel és korszerű vizualizációval tárja fel a támadási felületeket. Gyorsan azonosítja és hatástalanítja a sérülékenységeket, valamint orvosolja a megfelelőségi problémákat. A Skybox hatékonyabbá teszi a mindennapi védekezést a sérülékenységekkel szemben, miközben segíti a határvédelmet, a biztonsági házirendek kezelését és a fenyegetettségek elleni küzdelmet. Proaktív megközelítésének köszönhetően mérsékli napjaink biztonsági kockázatait még a világ legnagyobb szervezeteinél is.

SKYBOX™ SECURITY

Total Visibility. Focused Protection.™