secureVISIO

SecureVisio – egyetlen kiberbiztonsági platform az incidensek, sebezhetőségek és kockázatok észlelésére és kezelésére. A rendszerrel a szervezetek egyetlen integrált platformon automatizálhatják és egyesíthetik alapvető IT-biztonsági menedzsment műveleteiket. Ez lehetővé teszi számukra, hogy optimalizálják a biztonsági műveletek idejét és költségeit. **Az IT-biztonsági vezetők, CISO-k így jobb döntéseket hozhatnak, mivel teljes körű információik vannak az incidensekről, a sebezhetőségekről és a kapcsolódó kockázatokról egy helyen.**

A SecureVisio az eseménymenedzselési folyamat következő területeivel foglalkozik:

1

Helyzetismeret – az IT-eszközök és -folyamatok leltározása, feltérképezése, monitorozása

Az eszközök, hálózatok és folyamatok helyzetismeretének kialakítása a **biztonsági menedzsment** egyik legfontosabb feladata mind stratégiai, mind operatív szinten. A **SecureVisio automatizált** passzív és aktív IT-eszköz-leltárt és hálózati konfigurációs leképezési mechanizmusokat kínál. Ezek a mechanizmusok **észlelik** a rendszereket, hálózati eszközöket és alkalmazásokat, **automatikusan meghatározzák** azok típusát, valamint a köztük lévő kapcsolatokat. Lehetővé teszik azon **műszaki** és **üzleti folyamatok** azonosítását is, amelyekben az azonosított IT-erőforrások vagy IT-erőforrás-csoportok részt vesznek. A **leltározási folyamat** részeként a rendszer dinamikusan kiszámítja a lehetséges támadási vektorokat, és azonosítja az esetleges fenyegetéseket.

Az infrastruktúrát a hálózaton és a végpontokon alkalmazott **biztonsági intézkedések** szempontjából is elemzi. A modul összes eredménye egy vizualizált, interaktív, logikai **hálózati térkép** formájában jelenik meg.

Az összegyűjtött információkat más rendszermodulok használják fel:

- eseménykorrelációs paraméterként;
- az incidenskezelési folyamat részeként az incidenskörnyezet-adatok gazdagítására;
- a playbook kiválasztására és a szervizcsapatok feladatainak kiosztásához;
- az események prioritásainak befolyásolására;
- ez az automatizált kiberfenyegetések kockázatelemzésének alapja;
- befolyásolja a sérülékenységek rangsorolását és kezelését.

2

Kiberfenyegetések kockázatelemzése

A kiberfenyegetések **kockázatelemzése** stratégiai feladat a biztonságkezelési folyamatban. Ha egy vállalat tisztában van a kiberfenyegetésekkel kapcsolatos kockázatokkal, akkor hatékonyabban tudja kezelni őket. A kockázatelemzési folyamat által generált eredmények a **helyzetfelismerés** fontos részei, és hatással vannak az olyan operatív tevékenységekre, mint az incidensek és a sebezhetőség kezelési folyamatai.

A **SecureVisio** platform magában foglalja a folyamatok és IT-erőforrások automatizált, dinamikus kiberfenyegetési kockázatelemzésének mechanizmusait, amelyek az összegyűjtött és a leltári folyamat során **folyamatosan frissített** adatokon alapulnak. **Fejlett algoritmusok** elemzik a fenyegetés- és biztonsági mátrixokat, a támadási vektorokat, valamint a rendszerekre, folyamatokra és adatokra gyakorolt lehetséges következményeket. A kontextuális kockázatelemzési szabályokkal a kockázati mechanizmusok az egyes szervezetek **egyedi igényeihez** igazíthatók. Az **elemzési eredményeket** a grafikus kockázatelemző panel és a grafikus hálózati modell mutatja be. Ezenkívül fontos **eseménykorrelációs paraméterek** is befolyásolják az incidensek és a sebezhetőség prioritásait.

secureVISIO

3

SecureVisio SIEM

Eseményinformációk gyűjtése és tárolása

A **SecureVisio** hatékony, fejlett mechanizmusokkal van ellátva a **teljes informatikai** infrastruktúra eseményinformációinak összegyűjtésére és tárolására. A rendszer lehetővé teszi a naplók gyűjtését a **syslog protokollon**, a **Windows Event Forwarding** és az **API-**felületeken keresztül, valamint szöveges fájlok, adatbázisok, sőt e-mail-fiókok adatainak kiolvasását. Egy **fájlalapú adatbázist** használ, amely nagyon nagy teljesítményt tesz lehetővé. A beépített automatikus **archiválási mechanizmusok** hosszú távú, központi vagy elosztott adattárolást biztosítanak a rendszergazda által kiválasztott lemezköteten.

Események elemzése és összefüggései

A rendszer folyamatosan frissített **eseményelemző és -kezelő készlettel** van felszerelve a különböző adatforrások kezelésére. A **regex, xml, json,** feltételes és alárendelt elemzési mechanizmusok, a grafikus értelmező létrehozási felület, valamint a beépített hibakereső olyan hatékony eszközök, amelyek bármilyen forrásból származó adatok elemzésére és normalizálására képesek. A **normalizálási folyamat** az összegyűjtött adatokat kereshető és feldolgozható információkká alakítja át. A rendszerben megtalálhatók automatikus eseménykorrelációs mechanizmusok és folyamatosan frissített korrelációs szabályok, amelyek olyan mátrixokon alapulnak, mint a **MITRE ATT&CK**.

Fejlett, rendkívül rugalmas korrelációs motorja képes:

- események létrehozására más események alapján;
- incidensek létrehozására események alapján;
- prioritások meghatározására kontextus alapján;
- az erőforrásprofiloktól függő értékelési mechanizmus indítására;
- referenciatömbök létrehozására és azokra történő hivatkozásra;
- az incidensekhez kapcsolódó erőforrások (az erőforrás típusa és szerepe a szervezetben, a kockázatnak kitett műszaki és üzleti folyamatok, a feldolgozott adatok típusa, az incidens lehetséges következményei, támadási vektorok, kockázatelemzés eredményei) bevonására a kontextuskorrelációba;
- grafikus felületen történő megjelenítésre korrelációs szabályok létrehozásához.

4

SecureVisio SOAR

A biztonsági incidensek és sebezhetőségek kezelésére szolgáló folyamat megvalósítása

A **SecureVisio** platform egy fejlett **SOAR (Security Orchestration Automation and Response – biztonsági rendszerezési automatizálás és válaszadás)** modult tartalmaz. Ez lehetővé teszi a biztonságiincidens-kezelési folyamatok és eljárások megvalósítását az iparág legjobb gyakorlataival összhangban (mint az **ISO-270035, a NIST SP 800-61R2, az ENISA és a Carnegie Mellon Egyetem**). A **korrelációs mechanizmusok** által létrehozott minden potenciális biztonsági incidens egy folyamat részévé válik, amelynek során a **SecureVisio** automatikusan gazdagítja az adatokat, nyomon követi az állapotot, a válaszadási és kezelési időket, fokozza az incidenst, feltárja a lehetséges következményeket, és playbookokat biztosít az elemzés minden egyes szakaszának kezelésére, valamint a válaszfolyamatra.

Elemzési és eseményreakciós feladatok automatizálása

A **SecureVisio** a meghatározott paraméterek és az eseménykontextus alapján automatikusan feladatokat rendel a **SOC-csapat** mérnökeihez. A munkafolyamat az incidenskezelés minden egyes szakaszához **testre szabott playbookokat** követ.

4

A fejlett SOAR-funkciók közé tartozik:

- grafikus felület playbookok létrehozásához;
- lépésekre és szakaszokra bontott cselekvési tervek;
- interakció a végfelhasználókkal, kérdések feltevése és a további lépések válaszoktól függővé tétele;
- a playbook megváltoztatása vagy egy másik lépésre ugrás a körülmények alapján;
- beágyazott, automatikus vagy automatizált rendszerműveletek playbookokon belül;
- több playbook automatikusan alkalmazott állapottól, kontextustól és incidens/esemény paraméterektől függően;
- értesítés a szervizcsapatokról, valamint az erőforrás- és folyamattulajdonosokról meghatározott paraméterek, például erőforrástípus, kockázatnak kitett folyamatok, erőforrás fontossága, incidens/esemény prioritása alapján;
- értesítés, ha az incidens/esemény állapota megváltozik;
- értesítés a megállapított válasz- és szolgáltatási idők túllépéséről;
- az incidens/esemény prioritásától függő válaszadási és kezelési idő.

Az **incidenskezelési modul** előre beépített playbookokat és több száz műveletet tartalmaz, amelyek lehetővé teszik az automatikus vagy automatizált interakciót külső rendszerekkel az információgyűjtési, elforgatási és incidensreagálási folyamatok részeként.

Sebezhetőségkezelési folyamat megvalósítása

A sebezhetőségkezelési folyamat a biztonságkezelés egyik legfontosabb része. Éppen ezért a **SecureVisio** tartalmaz egy modult, amely átfogó megközelítést biztosít a sebezhetőségek kezeléséhez. A rendszer **integrációs interfésszel** rendelkezik a vezető sebezhetőség-ellenőrző technológiákkal. Ezek az interfészek lehetővé teszik a **sérülékenységvizsgálati** folyamat több szkenner használatával történő kezelését és az eredmények importálását.

A sebezhetőségkezelési alrendszeren belül a SecureVisio a következő feladatokat segíti elő:

- a sebezhetőségek rangsorolása más modulokból származó kontextuális adatok alapján;
- feladatok automatikus hozzárendelése a szolgáltatási csapatokhoz a kontextus alapján;
- sebezhetőség automatikus hozzárendelése, playbookok kezelése kontextus alapján;
- a szervizcsapatok, az erőforrás-tulajdonosok és a folyamattulajdonosok automatikus értesítése;
- a válaszadási és kezelési idők automatikus követése;
- automatikus eszkaláció;
- a sebezhetőségi információk gazdagítása más modulokból származó kontextuális információkkal.

5

Személyes adatok védelme

Az **Adatvédelmi modul** segítséget nyújt a szervezetnek az adatkezelési tevékenységekhez, feldolgozási kategóriák kialakításához és a jelentéstételhez.

A modul további funkciói:

- Keresés a személyes adatokat feldolgozó informatikai rendszerekben, valamint az ott kezelt adatcsoportokban és kategóriákban.
- A rendelkezésre álló, lehetséges fenyegetési források elleni műszaki biztosítékok meghatározása minden személyes adatokat feldolgozó informatikai rendszer esetében.
- „Adatvédelmi incidensről szóló jelentés” automatikus generálása a felügyeleti hatóság számára, beleértve a biztonság megsértése lehetséges következményeinek meghatározását.
- Az adatvédelmi hatásvizsgálat (kockázatelemzés) elvégzése a kiberbiztonsági fenyegetések körében – a GDPR előírásai szerint – teljesen automatizált módon.
- Automatikus elemzés az adatok elérhetőségének, bizalmasságának és integritásának elvesztési kockázatáról.
- A modulon belül feldolgozott információk további kontextust biztosítanak a kezelési folyamat során.