Astelia تضيف حجب مسارات الهجوم على مستوى الشبكة للثغرات غير المعالجة



أطلقت Astelia خاصية التخفيف الشبكي المستقل التي تحجب مسارات الوصول إلى الثغرات القابلة للوصول عبر قواعد WAF أو IPS/IDS، سواء توفر تصحيح أم لا، مع إمكانية التراجع والتسجيل.

- تحجب الخاصية مسار الشبكة إلى النظام الضعيف بدلًا من تعديل النظام نفسه.
- تعتمد على تحليل قابلية الوصول الذي يرسم طوبولوجيا الشبكة الفعلية وشروط كل استغلال.
- في أحد النشرات المؤسسية انخفض نحو 40 مليون ثغرة إلى أقل من 2,000 ثغرة قابلة للوصول.
- يشمل الدعم الأولي قواعد WAF وIPS/IDS، مع خطة لإضافة قواعد جدار الحماية.
- يمكن التراجع عن الإجراءات وتسجيلها ومراجعتها، مع إمكانية اشتراط موافقة بشرية لبيئات أو إجراءات محددة.

أعلنت Astelia عن خاصية التخفيف الشبكي المستقل، وهي موجهة إلى الفجوة بين سرعة الاستغلال المدعوم بالذكاء الاصطناعي وبطء دورات التصحيح. فبدلًا من تعديل النظام الضعيف، تحجب الأداة المسار الذي قد يسلكه المهاجم للوصول إليه.

آلية العمل

ترسم Astelia طوبولوجيا الشبكة الفعلية للمنظمة وتستخدم الذكاء الاصطناعي الوكيلي لتحديد ما يتطلبه كل استغلال. وبربط الأمرين تتبين الثغرات القابلة للوصول والمسارات المؤدية إليها. وفي إحدى النشرات المؤسسية انخفض نحو 40 مليون ثغرة إلى أقل من 2,000 ثغرة قابلة للوصول.

ولكل ثغرة قابلة للوصول تحدد الأداة نقطة اختناق فعالة على المسار وتطبق القاعدة هناك عبر WAF أو IPS/IDS لدى المنظمة. وقد تحمي قاعدة واحدة جميع الخوادم الضعيفة خلف هذه النقطة. أما قواعد جدار الحماية فمخطط لها ولم تدعم بعد.

الضوابط والحدود

تفيد الشركة بأن الأصل المحمي لا يتغير، ولذلك تبقى الأنظمة الحيوية، ومنها OT، قيد التشغيل، وأن الأسلوب يعمل حتى مع غياب التصحيح كما في الأنظمة المنتهية الدعم. ويمكن التراجع عن الإجراءات.

تحدد المنظمة الضوابط عبر Astelia Agents، ويمكنها اشتراط موافقة بشرية لبيئات أو إجراءات معينة، ويُسجَّل كل إجراء وتمكن مراجعته، وتستخدم الإجراءات صلاحيات محددة تفعّلها المنظمة. ويعمل التحليل عبر تكاملات للقراءة فقط.

هذه الادعاءات صادرة عن الشركة المطورة، لذا ينبغي التحقق منها في بيئتكم. ويناسب هذا النموذج الجهات التي يتعذر عليها التصحيح السريع بسبب نوافذ التغيير أو تأخر الموردين أو الأنظمة القديمة.

ما يجب فعله الآن

1. احصروا الأنظمة التي يصعب تصحيحها سريعاً، ومنها المنتهية الدعم وأصول OT، ووثّقوا الضوابط التعويضية لكل منها.
2. تحققوا مما إذا كانت WAF وIPS/IDS لديكم تقبل قواعد من أداة خارجية، ومن يعتمدها ضمن إجراءات إدارة التغيير.
3. عند تجربة أي أداة مماثلة، اشترطوا إمكانية التراجع وتسجيل كل إجراء وأقل الصلاحيات، وأبقوا الموافقة البشرية للبيئات الحرجة.
4. رتّبوا أولوية الثغرات وفق قابلية الوصول الشبكي إلى جانب درجة الخطورة، وتحققوا من النتائج على طوبولوجيا شبكتكم.
5. واءموا أي تخفيف شبكي مؤقت مع إجراءات إدارة الثغرات والتغيير وفق ضوابط ECC وإطار SAMA CSF، مع تحديد مسؤول وموعد مراجعة.