Euronext protege las operaciones financieras paneuropeas con Simulación de ataques (BAS) de Cymulate

Gracias a las evaluaciones multivectoriales, la plataforma permite al Departamento de Seguridad de la Información de Euronext comprobar la postura de ciberseguridad de la organización ante los últimos ciberataques y armonizar al mismo tiempo los esfuerzos de todos los equipos.

Organización

Euronext es el principal mercado de valores paneuropeo firmemente afianzado durante los cuatro siglos que lleva operando y que, actualmente, constituye una actividad clave en los mercados de capitales europeos. La bolsa de valores cuenta con 1300 empresas nacionales y extranjeras que cotizan, con una capitalización bursátil combinada de 3500 billones de euros.

Departamento de Seguridad de la Información de Euronext
El Departamento de Seguridad de la Información de Euronext se compone de varios equipos, entre ellos el equipo del Centro de Operaciones de Ciberseguridad (SOC) y el Equipo de Evaluación y Explotación. Si bien la misión principal del SOC tiene que ver con la respuesta a incidentes, la supervisión continua y la mejora de la postura de ciberseguridad de la organización, trabaja estrechamente con el Equipo de Evaluación y Explotación, que se encarga de ejecutar las evaluaciones de vulnerabilidades y del Red Team. El SOC es responsable de la seguridad de toda la infraestructura y los sistemas de Euronext, de todos los servicios y plataformas de operaciones bursátiles de Euronext, así como de todos los usuarios internos y externos, entre los que se incluye la propia bolsa de valores. El SOC trabaja ininterrumpidamente: 24 horas al día, 7 días a la semana.

Desafío empresarial

Siempre pendiente de los últimos avances en el mercado de la ciberseguridad, Jorge Ruão, responsable del Centro de Operaciones de Ciberseguridad de Euronext, buscaba métodos más eficaces de prevenir y detectar los ciberataques.
El Departamento de Seguridad de la Información tiene experiencia en desarrollar y ejecutar sus propias simulaciones de ciberataques para comprobar la postura de ciberseguridad de la organización frente a amenazas específicas.

Después de implementar tecnología nueva, desplegar una política de seguridad específica o actualizar el motor de reglas de una herramienta de ciberseguridad, los equipos realizaban simulaciones de ataques específicos para asegurarse de que podían ser bloqueados o, al menos, detectados y mitigados.

Aunque la práctica de ejecutar simulaciones de ataques es muy eficaz, desarrollar simulaciones de ataques específicos puede ser una tarea que requiere muchos recursos; todo depende de la complejidad de la cepa de malware en cuestión o de sus variantes asociadas.
«Esto es especialmente preocupante si el tiempo es crítico, por ejemplo», comenta Ruão, «cuando te enteras de que se está propagando por internet una nueva campaña de malware que explota vulnerabilidades Zero-Day y recién acabas de desplegar medidas de mitigación o de solución proporcionadas por los servicios de inteligencia».

Desafío
Euronext buscaba una forma más rentable de comprobar su postura de ciberseguridad que complementara las simulaciones de ciberataques desarrolladas manualmente por ellos mismos y que habían estado ejecutando hasta la fecha.

Solución
Al desplegar Cymulate, Euronext puede ejecutar rápidamente simulaciones de los últimos ciberataques con facilidad, y hacerlo de forma repetida y frecuente.

Ventajas
El equipo ahora puede determinar fácilmente el impacto de las nuevas tecnologías, las contramedidas de seguridad y los cambios de configuración, al tiempo que deja ver con claridad la efectividad de las decisiones empresariales adoptadas.

Solución

Impresionado por la facilidad de uso de Cymulate y su capacidad para ejecutar repetidamente la misma batería de pruebas para comprobar la postura de ciberseguridad de la organización, Ruão implementó la plataforma de simulación de ciberataques, con lo que eliminó la necesidad de desarrollar y preparar un marco manual para ejecutar esas mismas pruebas. Además de las pruebas de penetración manuales, los ejercicios de Red Team y las evaluaciones de vulnerabilidades que se realizan periódicamente, Cymulate permite al Departamento de Seguridad de la Información de Euronext realizar pruebas de ciberseguridad frecuentes en respuesta a distintos acontecimientos.

Por ejemplo, «cuando surge una nueva amenaza específica como WannaCry, etc., Cymulate incorpora los indicadores de compromiso (IoC) de la amenaza muy rápidamente», apunta Ruão, «y se puede ver de inmediato el grado de vulnerabilidad de la organización a esa amenaza sin necesidad de desarrollar internamente una simulación que imite esa nueva amenaza».
Del mismo modo, si una herramienta de seguridad de repente resulta menos eficaz tras un cambio de configuración, los ajustes se pueden actualizar y luego probar exhaustivamente ante toda una batería de ciberataques simulados.
Tras la adquisición de cuatro vectores de ataque (módulos) de Cymulate el año anterior, incluyendo los módulos de Evaluación Inmediata de Amenazas, Web Gateway, Email y Endpoint, Euronext ha renovado recientemente su suscripción a Cymulate e incorporado otro módulo más a la selección: Hopper, un vector que simula cualquier movimiento lateral potencial dentro de la red de la empresa. Acerca de la integración inicial, Ruão señala: «Fue muy fácil y rápido implementar la solución con resultados satisfactorios. No tuvimos ningún problema de importancia durante la implementación, aparte de tener que cumplir con los requisitos mínimos».

> *Personalmente, recomendaría Cymulate por su facilidad de uso, ya que puede proporcionar rápidamente información sobre el grado de vulnerabilidad o de protección de la organización ante las ciberamenazas externas.*
>
> Jorge Ruão, responsable de Operaciones de Seguridad de Euronext

Ventajas

Desde la implementación de la solución hace ya un año, tanto el equipo del SOC como el Equipo de Evaluación y Explotación utilizan Cymulate conjuntamente para averiguar y comprender si las contramedidas de seguridad actuales están realmente bloqueando las amenazas.
Gracias a Cymulate, el Departamento de Seguridad de la Información de Euronext ahora puede:

Probar los controles de seguridad contra las últimas amenazas: la plataforma simula los nuevos ataques inminentes que van surgiendo, lo que permite realizar evaluaciones de seguridad actualizadas.

Evaluar las contramedidas de seguridad con frecuencia y repetidamente: nuevas tecnologías, cambios de configuración o actualizaciones de software o hardware se pueden comprobar fácilmente para ver el impacto que tienen sobre la organización.

Complementar las simulaciones propias: aunque son muy eficaces, las simulaciones propias exigen muchos recursos y podrían no ser prácticas cuando el tiempo apremia.

Verificar el valor de las decisiones empresariales: al utilizar Cymulate como análisis comparativo (benchmark) antes de implementar una nueva tecnología, el equipo puede demostrar la eficacia de las nuevas soluciones.

Comprender el modus operandi de los ciberataques: esto incluye en qué eslabón de la Kill-Chain puede una amenaza potencial eludir con éxito las contramedidas de seguridad.

Permite la generación de informes ejecutivos y técnicos: Los informes internos proporcionan visibilidad sobre cómo contribuye cada tecnología a la postura de ciberseguridad global de la organización.

Desde la implementación de la plataforma, Ruão apunta que «estamos muy satisfechos con la solución Cymulate y ya estamos considerando ampliar sus funcionalidades con pruebas adicionales». En resumen, Ruão expresa que «Personalmente, recomendaría Cymulate por su facilidad de uso, ya que puede proporcionar rápidamente información sobre el grado de vulnerabilidad o de protección de la organización ante las ciberamenazas externas».

Oficina central: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | Oficina en EE. UU.: +1 212 6522632