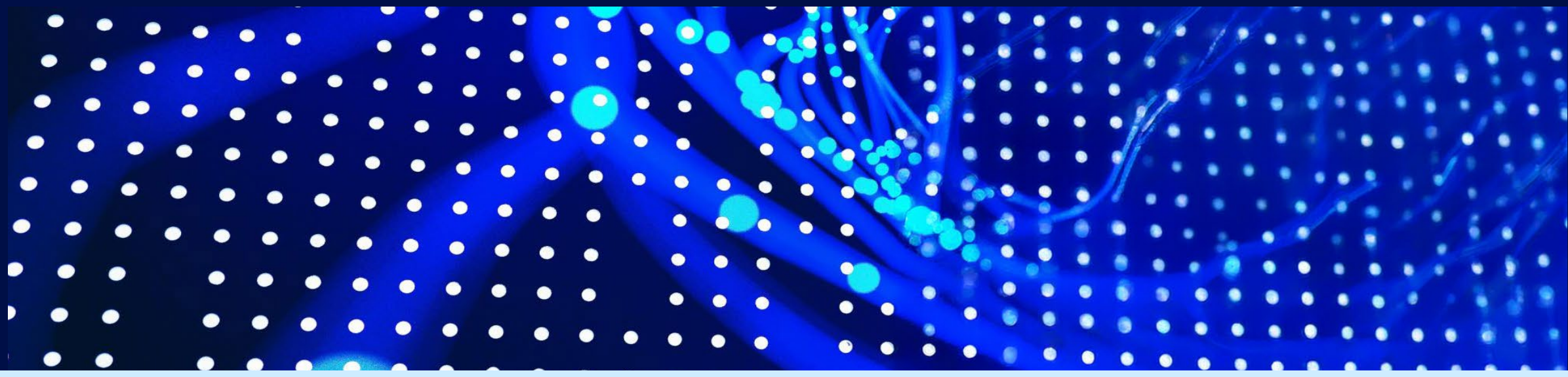
MARSH

Is your company really secure Challenging your technical controls with BAS



La IA aceleró el ataque y volvió insuficiente confiar en controles no validados. Esta sesión muestra cómo BAS y CTEM ayudan a probar defensas reales, identificar rutas explotables y movilizar remediación antes de que el atacante avance.

1

La IA cambió la velocidad del riesgo. Los ataques con IA crecieron 89% en 2025-2026 y el tiempo de ruptura más rápido observado fue de 27 segundos desde el acceso inicial hasta el movimiento lateral.

2

No asuma que sus controles funcionan: pruébelos. BAS valida continuamente EDR, firewall, SIEM, email, nube y red frente a TTPs reales, de forma segura y automatizada.

3

CTEM conecta diagnóstico y acción. Alcance, descubrimiento, priorización, validación y movilización permiten pasar de hallazgos técnicos a remediación priorizada por riesgo.

4

La identidad es una superficie crítica. 5 de las 10 principales tácticas MITRE están basadas en identidad; errores humanos, credenciales y configuraciones débiles pueden abrir rutas de ataque.

5

La dirección necesita métricas accionables. La validación continua permite reportar exposición, controles que fallan, avance de remediación y reducción de riesgo en lenguaje de negocio.