KANAN

ANÁLISIS DE ATAQUES Y BRECHAS

CÍRCULO DAAT

potencia tu información

Como respuesta a la creciente amenaza de ser afectados por los ciber incidentes, las organizaciones en todo el mundo han invertido una cantidad de recursos considerable, tanto tecnológicos como de capital humano, buscando implementar los controles que brinden seguridad a sus procesos y permitan alcanzar las metas establecidas para el negocio. A pesar de dichos esfuerzos en tiempo y recursos invertidos por las organizaciones, seguimos siendo testigos de brechas **que logran traspasar las defensas de las organizaciones de talla mundial a través de técnicas y/o ataques conocidos.** Entonces valdría la pena cuestionar ¿Dónde quedó la inversión en los controles de seguridad? o Los controles implementados, ¿son deficientes? La respuesta simple es que no existe un control capaz de asumir la protección adecuada para los activos críticos de una organización si no está configurado correctamente. Ahora bien: ¿Cómo logro identificar las fortalezas y debilidades de mis inversiones en seguridad?

Nuestra oferta de servicio de “Simulación de ataques y brechas” (BAS por sus siglas en inglés) va un paso más allá de lo tradicional, ya que el objetivo a evaluar son los controles tecnológicos que actúan como defensa de los activos de la organización (FWs, IPS, Proxies, Antispam, etc,), a diferencia del escenario típico en el que se invierte en un ejercicio de detección de vulnerabilidades en los activos, omitiendo los controles por los que el ataque debe atravesar para ingresar a la compañía objetivo.

Nuestro servicio de BAS valida la implementación de los controles y fácilmente identifica puntos débiles tales como protecciones configuradas deficientemente, permitiendo a la organización ajustar y cumplir sus objetivos tecnológicos:

EVALUA TUS PROTECCIONES

Verifica continuamente la efectividad de tus controles con ataques reales.

IDENTIFICA BRECHAS DE SEGURIDAD

Identifica brechas de seguridad en tiempo real y toma acción de inmediato para cerrarlas.

MAXIMIZA EL USO DE TU INFRAESTRUCTURA

Incrementa en semanas la efectividad de tus controles y mantén el nivel de protección.

EFICIENCIA OPERACIONAL

Identifica en tiempo real y ejecuta un plan de acción en minutos para la corrección de brechas de seguridad (parcheo virtual).

potencia tu información

SOLUCIONES KANAN / ANÁLISIS DE A&B

CÍRCULO DAAT

¿Cómo lo hacemos?

La solución está diseñada para detectar brechas o debilidades en los controles de seguridad gracias a un conjunto de 3 elementos:

- Atacante
- Víctima de Ataque
- Biblioteca de Ataques

Vector de ataque

Una vez determinado el alcance del servicio de BAS, se crean los **Vectores.** Un vector está compuesto de dos puntas: atacante y víctima y su finalidad es evaluar la postura de seguridad enfocándose en los controles tecnológicos involucrados, dependiendo el tipo de vector, los cuales pueden ser **Red, Endpoint y Correo electrónico.**

Atacante

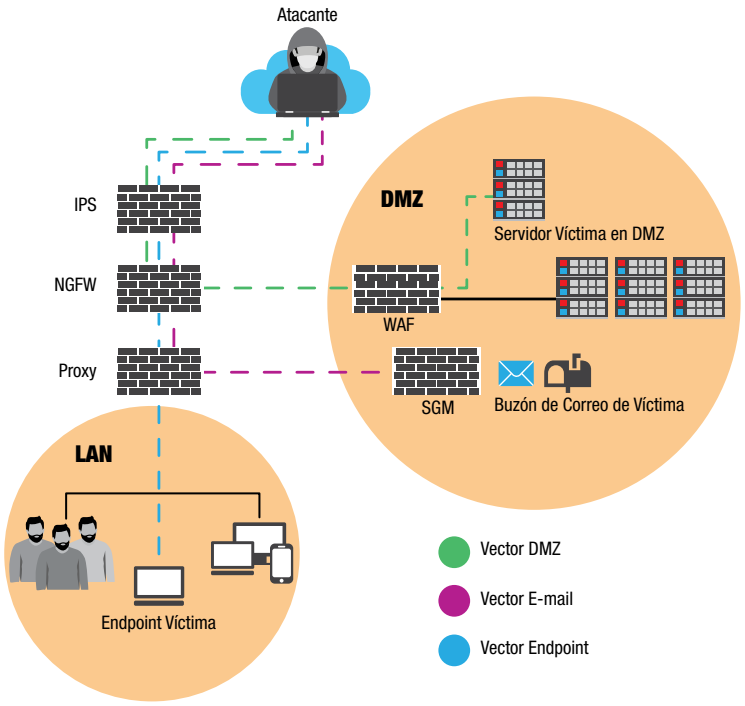
Los ataques se ejecutan desde un servidor en la nube, poniendo a prueba los controles tecnológicos involucrados en la postura de ciberseguridad de la organización, desde cualquier ubicación del mundo sin necesidad de usar tu infraestructura como atacante.

El servidor atacante consulta en la biblioteca las técnicas y mecanismos de ataque aplicables según el tipo de escenario, obteniendo así los ataques precisos a probar en tu infraestructura.

Víctimas de ataque

Los sistemas víctima de los ataques son el objetivo que busca alcanzar el atacante mediante el envío y ejecución de muestras de código malicioso, exploits, escenarios de ataques, además de simular brechas de datos mediante el uso de una biblioteca de muestras de exfiltración de datos de prueba. Cuando se determina el tipo de sistemas y aplicaciones cuyas defensas piensan ponerse a prueba, se despliegan los agentes que cumplirán el rol de victima según los escenarios de ataque a ejecutar: Endpoint, Red (DMZ y/o LAN) y Correo electrónico.

Representación de vectores de ataque

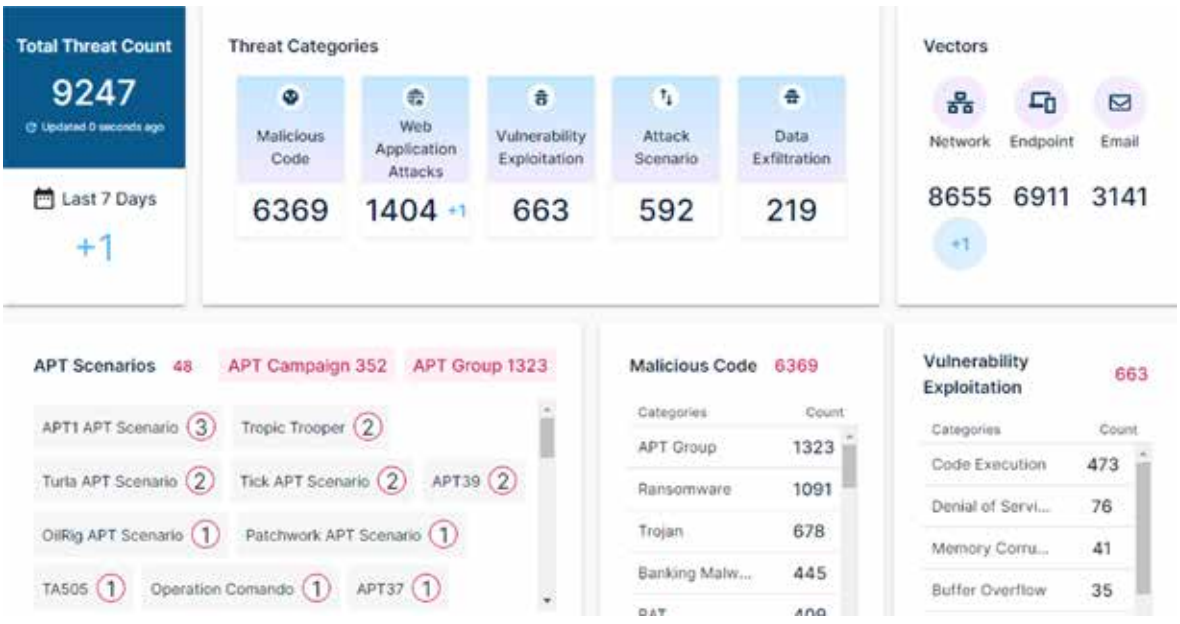


Biblioteca de ataques

La biblioteca contiene más de 9 mil ataques que van dirigidos a distintas tecnologías del mercado, dicha base de datos se actualiza de manera constante para estar al día con los más recientes ataques descubiertos en el mundo.

Cuenta con la capacidad para acotar los ataques a ejecutar permitiendo enfocar los esfuerzos a la infraestructura de mayor criticidad para la organización, puntualizando las tecnologías actuales del negocio.

Biblioteca de Ataques



SOLUCIONES KANAN / ANÁLISIS DE A&B

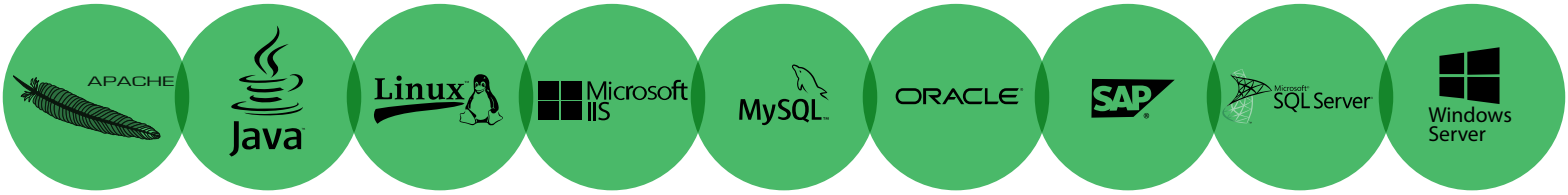
CÍRCULO DAAT

Alcance de los Servicios

Cada uno de los vectores pone a prueba tus controles de seguridad con base en diferentes alcances según el escenario de ataque.
Cabe resaltar que independientemente del vector, las pruebas realizadas no generan afectación alguna en tu infraestructura ni en tus usuarios.

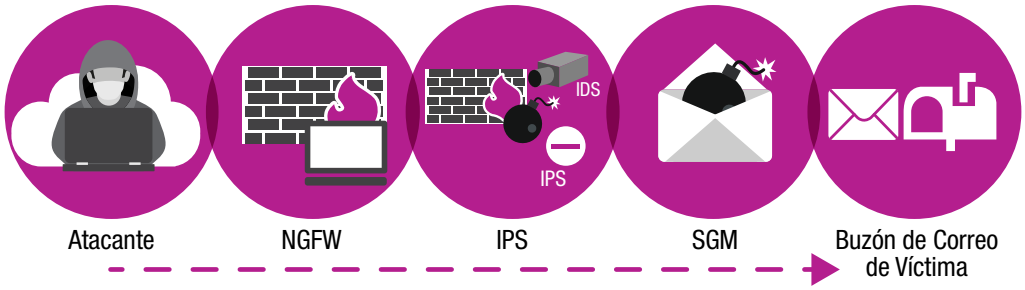
Vector de Red

Se aprovisiona un servidor virtual que toma el rol de víctima e independientemente del sistema o infraestructura de la empresa, recibirá los ataques de cada producto, sistema o escenario seleccionados dentro de biblioteca de ataques poniendo a prueba la efectividad de los controles involucrados,
Pone a prueba tus controles de seguridad tales como NGFW, IPS, WAF por las que un atacante debe atravesar para alcanzar y tomar control de tus activos críticos. Algunos de los productos objetivo de estos ataques simulados son:



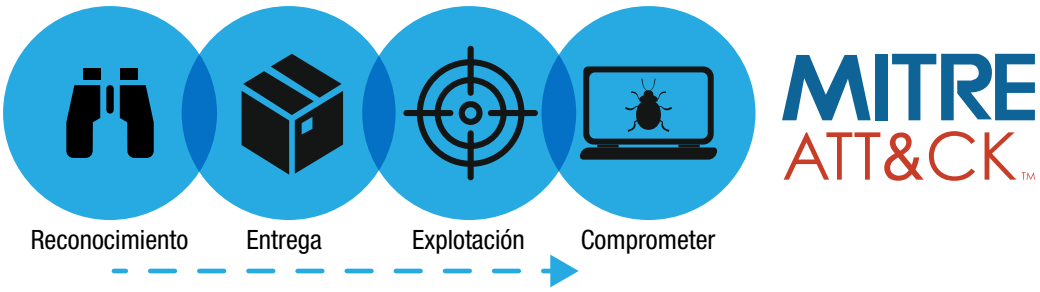
Vector de E-mail

Implementa las pruebas que te brindaran visibilidad real del estado de tus controles de seguridad en correo electrónico, independientemente de que tu solución de correo esté on-cloud u on-premise, mediante técnicas de entrega de amenazas reales y escenarios de robo de datos. Obtén certeza de tus controles contra malware, enlaces maliciosos, phishing y escenarios de exfiltración de datos en cualquier plataforma de correo.



Vector de Endpoint

Implementa un dispositivo final como si se tratara del equipo de un usuario y ejecuta pruebas en las distintas fases de ataque por las que atraviesa un atacante desde el reconocimiento hasta comprometer el sistema. Obtén priorización de resultados gracias al uso del marco de MITRE ATT&CK y define siguientes pasos para proteger los dispositivos finales:



Resultados

Obtén resultados puntuales dirigidos a la tecnología con la que se apoya la seguridad perimetral de la organización gracias a las alianzas que se tienen con las marcas líderes en el mercado:

Visibilidad directa de los puntos débiles de la implementación de tus protecciones, lo que permite identificar rápidamente el control que debe ser habilitado y con esto explota al máximo tu inversión.

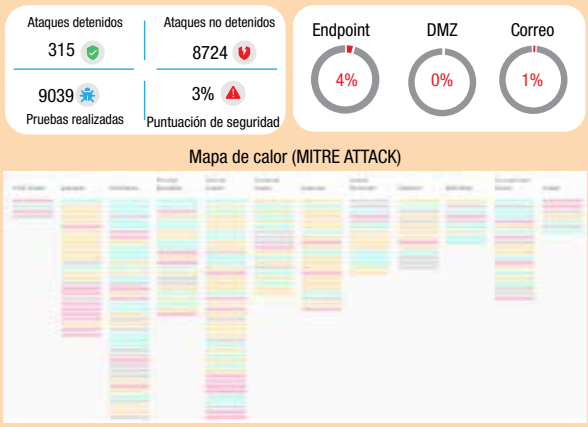
Check Point SOFTWARE TECHNOLOGIES LTD. · cisco Firepower · F5 · FORTINET · McAfee · paloalto NETWORKS · SNORT

SOLUCIONES KANAN / ANÁLISIS DE A&B

CÍRCULO DAAT

Obtén resultados entendibles y accionables gracias al uso de marcos de trabajo y metodologías conocidas, además de semáforos y KPIs que permitirán trazar correctamente el avance obtenido en un periodo.

Obtén el acompañamiento de nuestro grupo de expertos que ayudarán a traducir los hallazgos y recomendaciones en un plan de acción digerible y eficiente para tu organización.



Modelo de servicios

Obtén certeza y desaparece el falso sentido de seguridad, valida el crecimiento de tus controles de seguridad y logra un monitoreo único en el mercado que compara tus protecciones perimetrales contra las crecientes amenazas en internet que surgen día tras día con los siguientes modelos de servicio:

Análisis en un solo evento - Cobre

Evalúa e identifica brechas en los controles de seguridad para uno o más vectores, obtén el reporte ejecutivo con semáforos de hallazgos, el reporte técnico con el detalle, así como información puntual para lograr la remediación y una presentación de resultados.
Tiempo estimado de resultados: 2 semanas

Evaluación y validación posterior - Bronce

Evalúa e identifica brechas en los controles de seguridad para uno o más vectores. Se obtendrán los reportes ejecutivos y técnicos, así como la presentación de resultados y una vez obtenidos los hallazgos fortalece tus controles para someterlos a una 2da revisión de seguimiento (en menos de 30 días) que incluye la entrega de reportes ejecutivos y técnicos incluyendo cambios detectados y comparación de resultados.
Se estima un tiempo de 2 semanas por evento (Inicial y revisión).

Análisis periódico con mejora continua – Plata / Oro

Obtén reportes periódicos establecidos mediante un contrato mensual (flexible) en un esquema de mejora continua, vigila, monitorea y mide que cualquier cambio en las configuraciones mantenga la protección para la que fue pensado o detecta cualquier brecha abierta después de modificar nuevas políticas de control en la organización.
Compara el crecimiento en eficiencia de tus inversiones de seguridad y vuelve le mejora de tus controles una constante.

NIVEL DE SERVICIO	COBRE	BRONCE	PLATA/ORO
IDENTIFICACIÓN	✓	✓	✓
EVALUACIÓN	OPCIONAL	✓	✓
PROTECCIÓN	OPCIONAL	✓	✓
VALIDACIÓN DE PROTECCIONES	–	✓	✓
MONITOREO Y MEJORA CONTINUA	–	–	✓

CENTRO
Filadelfia 128, Oficina 602
Col. Nápoles
Alcaldía Benito Juárez
México CDMX 03810

CONMUTADOR
+52.55.5202 5010
comercial@circulodaat.mx
circulodaat.mx

NORTE
+52.81.4159 0580
Penthouse 1, Edificio III Moll del Valle
Calzada del Valle 400
Col. Del Valle
San Pedro Garza, García