Documento técnico

Tecnología del engaño

Una parte integral del SOC de próxima generación

Resumen ejecutivo

Con la mejora de las capacidades de los adversarios, mayores intereses que nunca en torno a la seguridad de la información y un panorama de amenazas en rápida evolución, todos quieren un SOC de próxima generación. Pero, ¿qué significa eso realmente?

En su forma más básica, implica evolucionar de casos de uso de detección estática y agregado de registros simples a un modelo proactivo de detección de falsos positivos bajos, con análisis profundo para convertir datos en información y, finalmente, mecanismos de respuesta altamente automatizados.

La tecnología del engaño proviene de un estudio del punto de vista del atacante y, en consecuencia, equipa a los equipos de operaciones de seguridad con muchas de las capacidades más deseadas de un SOC de próxima generación.

Este documento técnico ilustra algunas de las formas clave en que puede actualizar sus capacidades de supervisión con el engaño para frustrar las amenazas de manera más rápida, precisa y con mayor confianza.

La tecnología del engaño proviene de un estudio del punto de vista del atacante y, en consecuencia, equipa a los equipos de operaciones de seguridad con muchas de las capacidades más deseadas de un SOC de próxima generación.

Tema clave

- Los centros de operaciones de seguridad deben "asumir la infracción" y trabajar como si el entorno ya estuviera comprometido para encontrar amenazas avanzadas.
- Las defensas proactivas como el engaño y la caza de amenazas dan la vuelta a la situación, ya que le trasladan al atacante los costos económicos, de tiempo, de recursos y cognitivos. Deben trabajar duro para evadir la detección, en lugar de que el equipo de seguridad trabaje duro para detectarlos.
- Los falsos positivos y los datos incorrectos son la pesadilla de la mayoría de los SOC actuales. El engaño tiene la tasa de falsos positivos más baja de cualquier clase de solución, ya que cualquier interacción con un activo engañoso es sospechosa.
- Con un bajo número de falsos positivos, los equipos de seguridad pueden orquestar su respuesta a los incidentes, sin necesidad de intervención humana.
- Los activos engañosos solo atraen interacciones malas o anómalas, por lo que el análisis de datos se puede usar para obtener una mejor perspectiva, crear inteligencia de amenazas y responder más rápido.
- El engaño es una capacidad, no un producto o tecnología. Implica capacitación, procesos y una estrategia de engaño que están basados en el riesgo y vinculados a los imperativos comerciales.

He aquí un desglose de las 6 RAZONES PRINCIPALES por las que una plataforma de engaño es un componente crucial del SOC de próxima generación:

1 **Asumir el incumplimiento**

Ya quedó atrás esa época (si es que alguna vez existió) en la que los defensores podían dividir claramente su red en zonas confiables y no confiables. Dado que las redes escalan y las capacidades de los adversarios se mantienen muy por delante de las capacidades del equipo de seguridad promedio, el sector está comenzando a asumir que el entorno es hostil y que es probable que ya se haya iniciado alguna fase de compromiso.

Este enfoque libera a los defensores de tener que tratar de ocultar cada debilidad (una tarea imposible) para establecer una línea de base y supervisar el compromiso en curso. Si los equipos de seguridad tienen una buena línea de base y una telemetría confiable, pueden encontrar incluso a los atacantes más sofisticados que habitan dentro de la red.

La tecnología del engaño ya "asume el incumplimiento". Se colocan señuelos en puntos finales, en Active Directory y en la red, de tal manera que un atacante en curso interactúe con estos activos engañosos y revele su presencia.

2 **Defensa proactiva**

La tecnología del engaño es una "defensa activa" diseñada para hacer que la red sea hostil para los atacantes y trasladarles los costes de permanecer sin ser detectados. Por el contrario, los casos de uso de supervisión de seguridad estática se vuelven obsoletos rápidamente y no pueden mantenerse al día con las tácticas cambiantes de los atacantes, lo que facilita que los atacantes evadan la detección y permanezcan dentro de la red durante meses o incluso años.

Sin embargo, el engaño no se basa en casos de uso estáticos. Al centrarse en la intención de las personas que están detrás de un ataque, en lugar de en las herramientas, vulnerabilidades o www.smokescreen.io techniques que se utilizan, las defensas basadas en el engaño pueden seguir siendo efectivas sin importar lo que los ciberdelincuentes intenten en el futuro. Esto significa que el SOC moderno puede mantenerse ágil y adaptable a las nuevas amenazas sin tener que esperar para verlas primero. Los cazadores de amenazas y los responsables de responder a incidentes también pueden utilizar el engaño para tender trampas tanto para encontrar los focos de mal como para dimensionar la propagación de un incidente en curso.

3 **Falsos positivos bajos**

Los SOC tradicionales han "dado la voz de alarma" con demasiada frecuencia. Incluso con un ajuste significativo, encontrar el equilibrio entre demasiadas alertas y pasar por alto incidentes reales es un proceso extremadamente complicado y constante. Una reducción en la cantidad de falsos positivos automáticamente hace que el equipo de seguridad sea más productivo, ya que puede centrarse en amenazas reales en lugar de perseguir algo que no existe.

La tecnología del engaño tiene un número extremadamente bajo de falsos positivos porque nadie debería siquiera interactuar con un sistema, una credencial o un archivo de señuelo. Cualquier interacción es digna de investigación e incluso puede desencadenar una respuesta orquestada. Esto significa que el SOC puede reducir la cantidad de alertas a solo las que importan.

4 **Análisis de datos e inteligencia de amenazas**

La mayoría de los análisis de datos se centran en "recopilar todo" y luego tratar de dar sentido a los datos. La seguridad no es necesariamente un problema de big data, es más un problema de "buenos datos". Dado que los sistemas de engaño solo ven tráfico anómalo o malicioso, se pueden aplicar análisis de datos para comprender mejor las amenazas dentro de la red en lugar de buscar una aguja en un pajar (o en ElasticSearch DB).

Esto también significa que el SOC puede pasar de consumir inteligencia de amenazas externa estática (que no es específica y, a menudo, obsoleta) a crear su propia inteligencia de amenazas e IOC, que son más relevantes para la empresa y pueden informar mejor sobre defensas futuras.

5 **Respuesta orquestada**

Para hacer frente a las amenazas a la velocidad necesaria, se precisan mecanismos de respuesta orquestados. Sin embargo, el desafío es encontrar elementos que activen la orquestación que sean lo suficientemente confiables para que un ser humano no tenga que validarlos antes de que se dispare la respuesta. No hacerlo puede significar que las acciones de respuesta desencadenen falsos positivos, lo que puede conducir a la interrupción de la actividad comercial legítima.

Con un bajo número de falsos positivos y capacidades integradas de orquestación e integración, una plataforma de engaño puede permitir una "respuesta continua", detectando de manera confiable activos y usuarios comprometidos dentro de la red, e investigando, conteniendo o erradicando la amenaza automáticamente, sin necesidad de intervención humana.

6 **Amenazas internas**

Si bien los equipos de seguridad generalmente se han centrado más en los adversarios externos, las amenazas internas con acceso legítimo son mucho más difíciles de abordar. Suelen tener un conocimiento detallado de los mecanismos de seguridad implementados y pueden adaptar su intención maliciosa para que parezca completamente benigna.

El engaño puede detectar amenazas internas que buscan datos sobre personal objetivo de alto valor, buscan sistemas a los que no deben acceder, o copian y abren datos para los que no están autorizados. También introduce un elemento de imprevisibilidad; los despliegues de engaño son invisibles para los usuarios normales y la ubicación de los señuelos solo la conoce un círculo de confianza limitado, por lo que la persona que supone un peligro interno no sabrá de la existencia ni la ubicación del engaño. Esto también sirve como elemento disuasorio contra el fraude casual o la curiosidad fuera de lugar por parte de los empleados internos.

Detectar usuarios comprometidos

Detener el movimiento lateral

Interrumpir el ransomware

El engaño es un componente crucial del SOC moderno. El uso del pensamiento similar al de los adversarios a la hora de luchar contra el atacante cambia las normas del juego para los defensores, permitiéndoles "golpear por encima de sus posibilidades" a los adversarios sofisticados.

La tecnología de engaño de Zscaler Deception ha ayudado a algunos de los equipos de supervisión de seguridad más maduros del mundo a llevar sus capacidades de detección y respuesta al siguiente nivel, y ha permitido que nuevos equipos de seguridad comiencen a defender sus redes contra amenazas específicas con mayor fidelidad, productividad, automatización y confiabilidad.

zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.es