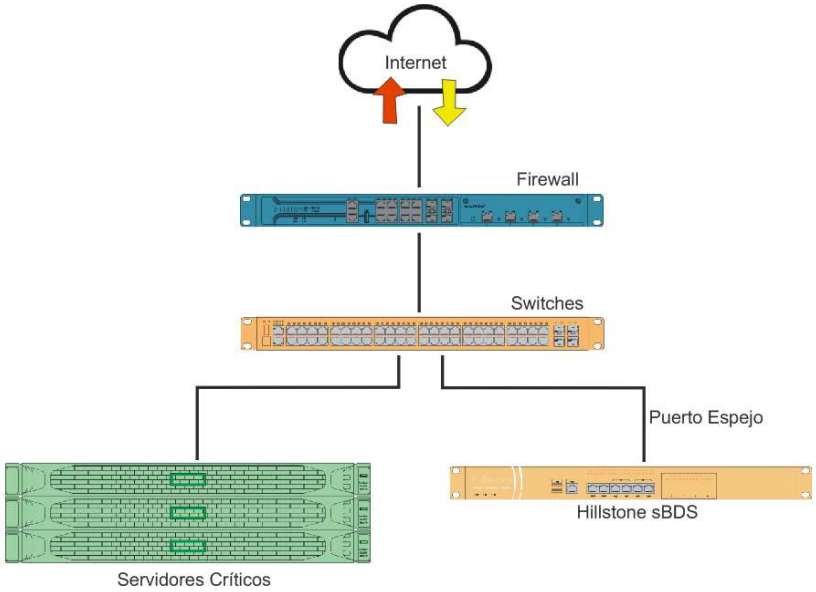
PROTECCION PARA SERVIDORES

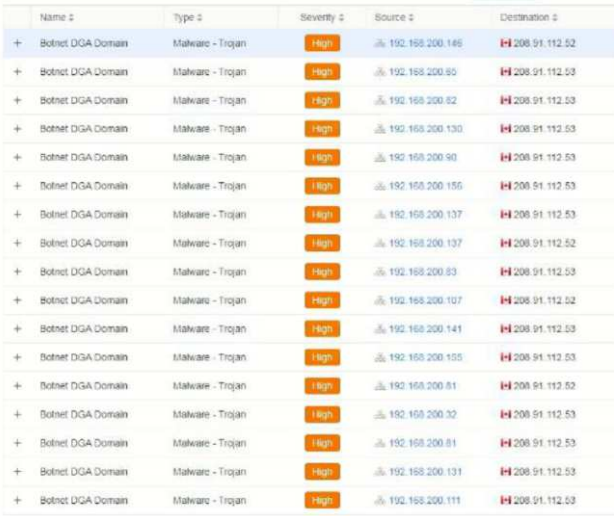
Servidor de Detección de Brechas sBDS

Proteja sus aplicaciones y servidores críticos de las amenazas más recientes con visibilidad y eficacia incomparables.



La tecnología de detección de brechas sBDS (Server Breach Detection System) de Hillstone Networks, ayuda en la detección de amenazas avanzadas dentro de la red, en servidores y hosts críticos, utilizando tecnología en el análisis y modelado inteligente del tráfico en tiempo real y comportamientos anormales dentro de la red.

Con esta tecnología se descubren de forma temprana las amenazas de próxima generación que fácilmente pueden evadir la detección perimetral (Firewalls) no importando si estos son dispositivos altamente sofisticados y de tecnología reciente.



Por otro lado, ayuda a mitigar estas amenazas (de múltiples etapas y capas) cuando ya están activas en la red con tecnología sofisticada construida sobre la bien aceptada cadena Cyber Kill Chain y los marcos de trabajo MITRE ATT & CK en evolución.

El Servidor de Detección de Brechas se vale de tres tecnologías:

I. Utiliza el agrupamiento estadístico para detectar brechas de seguridad en tiempo real, dándole prioridad a los hosts que tienen un nivel de riesgo alto y ofrece información de contexto sobre los ataques.

II. Utiliza análisis de comportamiento para detectar conductas anómalas en la red. El equipo ofrece visibilidad en cada una de las etapas de un ataque y le da al usuario múltiples oportunidades para detenerlos.

III. Proporciona un análisis forense para que el administrador pueda determinar la causa raíz del ataque. Esto le permite efectuar cambios en las políticas o reglas de seguridad informática en su red para prevenir situaciones similares

I-1850

I-2850

I-3850

I-5850

Seis propuestas de valor del sBDS de Hillstone

1. Protección Integral de los Servidores

Hillstone sBDS realiza el monitoreo en tiempo real de servidores críticos y estaciones de trabajo que contienen datos confidenciales o ejecutan servicios importantes, detectando vulnerabilidades desconocidas y ataques de día 0 que ya estén sembrados.

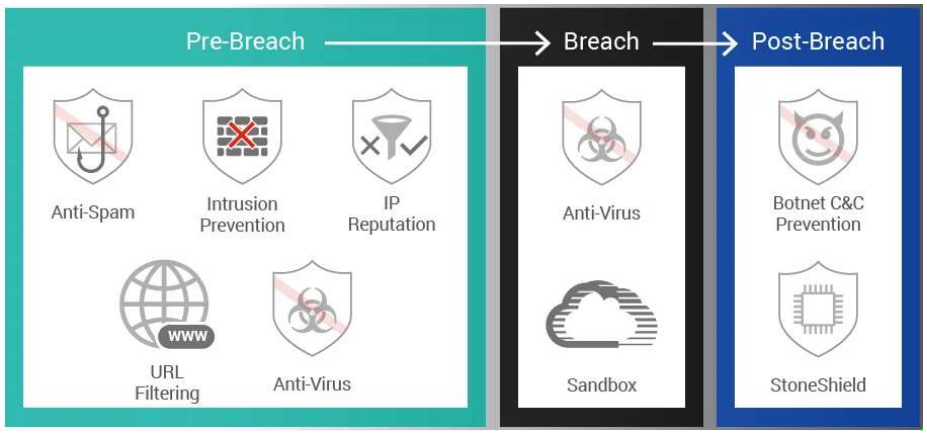
La detección de comportamiento anormal, la detección avanzada de amenazas y el uso de tecnología de engaño permiten que el sBDS descubra estas amenazas desconocidas para los servidores de la organización.

Una vez que el dispositivo detecta un comportamiento anormal, el sBDS de Hillstone realizará el análisis de la amenaza, mostrando con el uso de gráficos una amplia visibilidad de lo encontrado, Esto da información sobre el progreso del ataque, tendencias, así como toda la evaluación de riesgos.

Utiliza también, herramientas prácticas como el Índice de Reputación del Comportamiento y el Índice de Salud de la Red que ayudan a los administradores a maximizar la seguridad de TI.

2. Correlación integral de amenazas, análisis y detección

Los ciber-atacantes se han vuelto cada vez más sofisticados, utilizando ataques dirigidos, persistentes, sigilosos y de múltiples fases, que puede evadir fácilmente la detección perimetral. El sBDS de Hillstone consta de múltiples motores de detección enfocados en diferentes aspectos del descubrimiento de amenazas posteriores a la transgresión, incluido el malware avanzado detección (ATD), detección de comportamiento anormal (ABD), también como motores tradicionales de detección de intrusos y detección de virus.



La plataforma de correlación de amenazas de Hillstone analiza los detalles y relaciones de cada evento de amenaza sospechosa individual, así como información contextual dentro de la red, para conectar los puntos y proporcionar información precisa y efectiva para la detección de ataques con altos niveles de confianza.

3. Indicador de compromisos

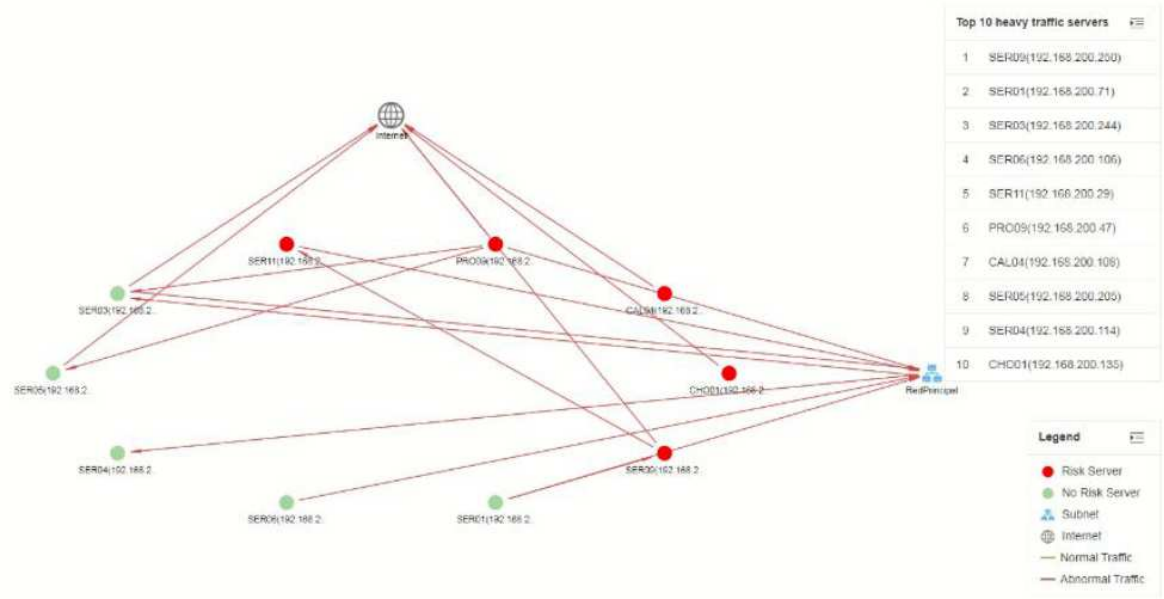
Los Indicadores de Compromiso (IoC) generalmente se consideran actividades de amenaza con mayor riesgo y con un alto nivel de confianza comprometido y representan una amenaza potencialmente mayor para los activos críticos dentro de la red.

Los eventos de IoC son eventos de amenazas detectadas durante el ataque posterior a la transgresión. Se identifican entre un gran número de ataques y amenazas en la red que están directamente asociados con el servidor o host protegido.

Detectar de manera efectiva y realizar una detección profunda de amenazas en estos Indicadores de Compromiso (IoC) es fundamental para limitar la vulnerabilidad de servidores y la filtración de datos importantes y evitando así, que una amenaza se propague aún más dentro de la red.

4. Visibilidad total de amenazas en curso y detalle de Cyber Kill Chain

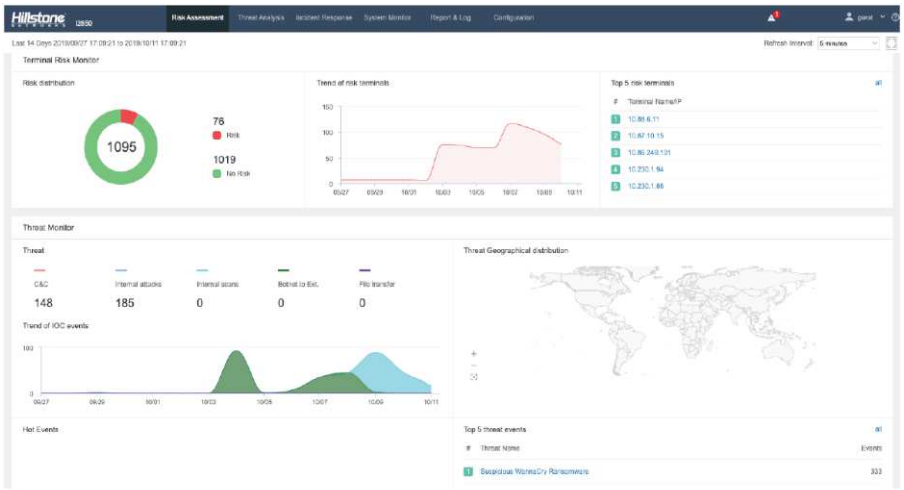
El SBDS de Hillstone proporciona visibilidad de los indicadores de compromiso (IoC) en curso reconstruyendo la cadena de ataque Cyber Kill y correlacionando eventos dentro de los espectros de tiempo y espacio.

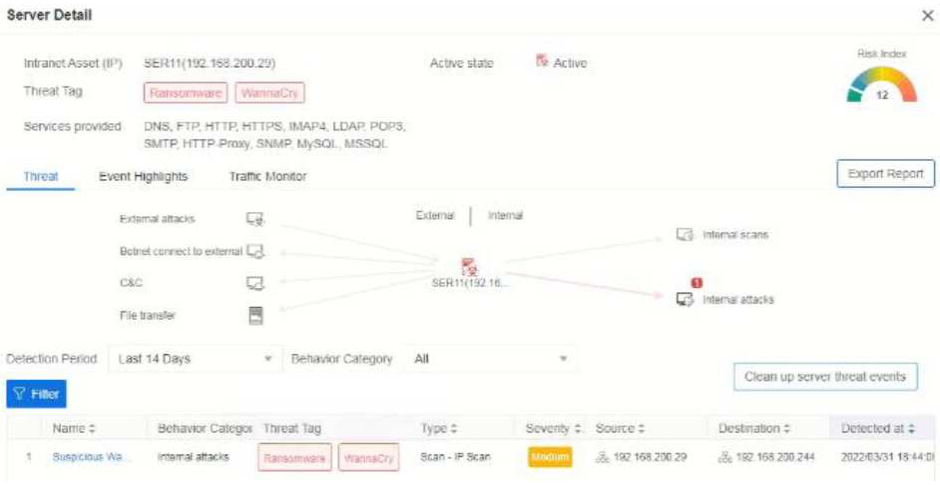


Además, proporciona monitoreo del tráfico del servidor y mapeo de patrones de tráfico para que las fuentes de amenazas u otros sistemas comprometidos en sentido descendente se puedan catalogar fácilmente. Las capacidades forenses integradas facilitan el aprendizaje del sistema para identificar los vectores clave de compromiso y bloquearlos en el futuro.

5. Alta eficacia con falsos positivos

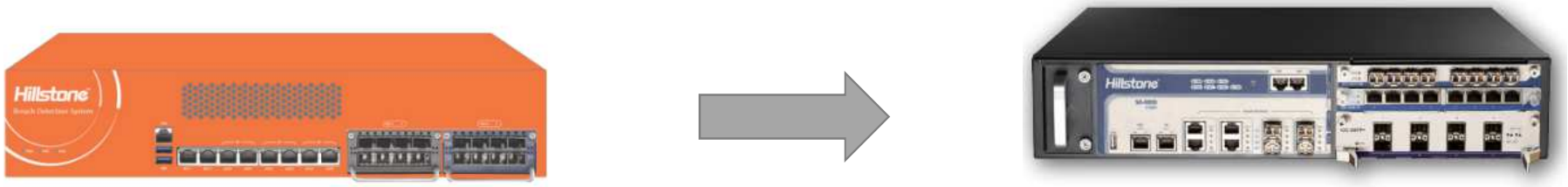
El uso de análisis de correlación avanzados en diferentes indicadores de compromiso (IoC) permite que el sBDS de Hillstone detecte y muestre amenazas reales (Pocos Falsos Positivos) sin abrumar a los administradores de redes, de por sí ya ocupados, lo que mejora la confianza en la solución y da como resultado acciones que mejoran la seguridad.





6. Integración con Hillstone Suite

La plataforma Hillstone sBDS realiza mitigación de amenazas con conjunto con los equipos Hillstone Firewalls E-Series NGFW, IPS NGIPS o T-Series iNGFW, que se implementan en el perímetro de la red.



Después de que el administrador de seguridad o los operadores de red analizan y validan las amenazas detectadas en el sBDS, pueden agregar elementos de amenaza como direcciones IP, tipo de amenazas, entre otros, a la lista negra o políticas de seguridad y luego sincronizarlos con los firewalls de Hillstone para que futuros ataques queden bloqueados en el perímetro de la red, esto evita futuros ataques y propagación a otros lugares de la red.

¿Quiénes Somos?

Raudo Networks S.A. de C.V. somos una empresa mexicana formada por ingenieros empeñados en solucionar problemas de tecnologías de la información y seguridad.

Trabajamos principalmente en el ramo de la ciberseguridad e infraestructura de TI, con el fin de mejorar la operación, incrementar la confiabilidad y la productividad de los sistemas informáticos de nuestros clientes.

Contacto:

sales@raudonet.com

+52 55 9052 8238

www.raudonet.com

Eugenia 413, Del Valle, Benito Juárez, CP 03100, CMDX, México