FORCEPOINT

Datasheet

UEBA DE FORCEPOINT

Seguridad de la información

PROTEGER LA IP, DETECTAR LAS CUENTAS COMPROMETIDAS Y REDUCIR EL RIESGO DE AMENAZAS INTERNAS

El Análisis de Comportamiento de Usuarios y Entidades (UEBA) de Forcepoint permite a los equipos de seguridad monitorear en forma proactiva los comportamientos de alto riesgo dentro de la empresa. Nuestra plataforma de análisis de seguridad proporciona un contexto sin igual al fusionar los datos estructurados y no estructurados para identificar e interrumpir a los usuarios maliciosos, comprometidos y negligentes. Descubrimos problemas críticos como cuentas comprometidas, espionaje corporativo, robo de propiedad intelectual y fraude.

POR QUÉ APLICAR EL UEBA de FORCEPOINT PARA LA SEGURIDAD

Nuestros clientes confían en nosotros para que les brindemos contexto sobre el comportamiento humano dentro de la empresa. Solo el UEBA de Forcepoint ofrece un análisis configurable para ayudar a los analistas de seguridad a enfrentar los problemas más importantes de la empresa. Proporcionamos la opción de ampliarnos a la vez que ayudamos a los equipos de seguridad a:

- Reducir el tiempo para detectar ataques de internos
- Destacar las alertas relevantes cuando los equipos de seguridad se enfrentan a diversos problemas.
- Realizar controles granulares sobre la actividad interna, más allá de SIEM y otras herramientas de su sistema
- Mejorar la eficiencia de las investigaciones para la respuesta ante incidentes y el análisis forense posterior a una filtración.

PILARES DE LA PLATAFORMA

Forcepoint UEBA proporciona conocimiento sobre comportamientos y personas de alto riesgo, no solo alertas sobre actividades anómalas. Al evaluar los aspectos de las interacciones entre personas, datos, dispositivos y aplicaciones, el UEBA de Forcepoint prioriza los cronogramas para los equipos de seguridad. Nuestro software se creó sobre cuatro pilares:

Contenido enriquecido › Fusiona las distintas fuentes de datos en una única narrativa, que combina el contenido de las comunicaciones para descifrar la intención junto con SIEM (Gestión de Información y Eventos de Seguridad) y fuentes (feeds) enriquecidas de los dispositivos finales y los empleados.

Análisis conductual› Aplica varios tipos de análisis estrictos de comportamiento y basados en el contenido enfocados en la detección de cambios, patrones y anomalías para detectar mejor los ataques sofisticados.

Ejemplos clave de uso

- **Actividades de los precursores**
- **DLP sensible al contenido**
- **Detección de cuentas comprometidas**
- **Reconocimiento de datos**
- **Abuso de usuarios con privilegios**
- **Análisis de seguridad**

Búsqueda y descubrimiento › Expone herramientas de descubrimiento y búsqueda forense poderosas a través de una interfaz de usuario con gran contexto para el monitoreo constante y las investigaciones exhaustivas.

Flujo de trabajo intuitivo › Ofrece informes proactivos que se integran completamente con el flujo de trabajo humano y la arquitectura de información del cliente existente para optimizar la eficiencia operativa.

REDEFINICIÓN DEL ANÁLISIS DE SEGURIDAD

Visibilidad impulsada por el contexto › El UEBA de Forcepoint ofrece de manera exclusiva visibilidad de las actividades, el comportamiento y las relaciones de los empleados al integrar flujos de datos no estructurados de gran contexto con datos estructurados. Nuestros modelos analíticos permiten calificar y priorizar entidades y eventos a través de varias perspectivas en todos los caudales de datos, algo que anteriormente no estaba disponible para los equipos de seguridad. También nos integramos con Active Directory, SIEM, EDR y fuentes de datos clave para ofrecer un verdadero conocimiento de la situación, y una plataforma forense poderosa que mejora drásticamente las investigaciones internas.

Análisis configurable › Las herramientas UBA tradicionales tipo caja negra a menudo están limitadas a fuentes de datos estructuradas, se analizan en distintos sistemas y tienen una configuración fija para el análisis. El UEBA de Forcepoint, por el contrario, ofrece capacidades de análisis poderosas que permiten a los equipos de seguridad abordar casos de uso de seguridad en desarrollo, y realizar un análisis ad-hoc en tiempo real, incluida la búsqueda avanzada en todos los conjuntos de datos. Nuestros análisis se pueden ajustar sin la necesidad de programación adicional, lo que permite una respuesta más veloz ante amenazas de seguridad.

Escala › Fundamentalmente, brindamos la posibilidad de ampliarnos. Solo el UEBA de Forcepoint utiliza ElasticSearch para facilitar un acceso instantáneo a enormes cantidades de datos. Nuestra plataforma almacena sin inconvenientes datos estructurados y no estructurados y permite ampliarnos en forma horizontal para crecer con nuestros clientes. El UEBA de Forcepoint también proporciona niveles variables de acceso y controles administrativos, para que confíe en que nuestra tecnología servirá a los fines de su empresa en cualquier tipo de implementación.

Capacidades

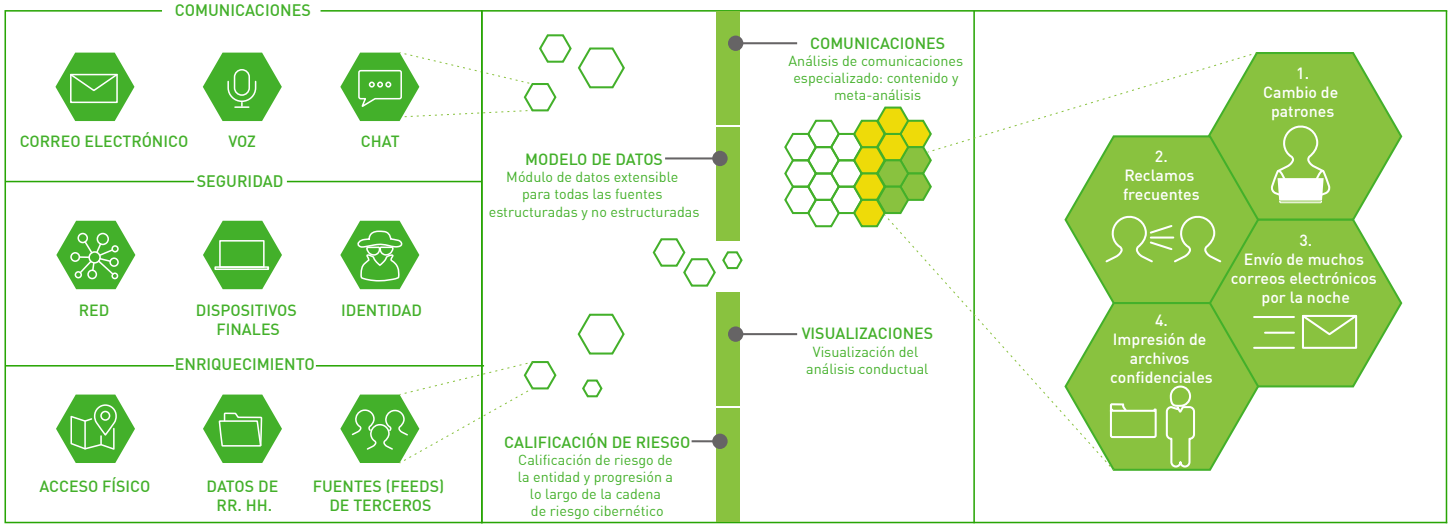
- **Tableros de control y flujos de trabajo basados en los roles** Facilitan la revisión rápida de la actividad que no cumple con las políticas a través de una interfaz de usuario intuitiva de modo que los analistas y gerentes puedan investigar, revisar, escalar y tomar medidas rápidamente.
- **Privilegios de datos sólidos** Soporte completo para los privilegios de datos complejos requeridos por los controles internos y problemas de privacidad externos.
- **Plataforma extensible** Análisis configurable, paneles de control configurables y casos de uso de seguridad inmediata de soporte de flujo de trabajo con capacidad completa para ampliarse a cualquier caso de uso de riesgo. Ofrece modelos científicos de datos avanzados sin tener que comprometerse a servicios profesionales estrictos.
- **Opciones de implementación flexible** Implementa el UEBA de Forcepoint de inmediato en las instalaciones, en una nube virtual o incluso al utilizar un dispositivo de UEBA.

Análisis avanzado

- **Análisis del comportamiento** Identifica cambios en el comportamiento que pueden indicar una actividad no deseada o no conforme, actual o potencial, por parte de los empleados mediante el análisis de comportamiento y contenido.
- **Priorización inteligente** Prioriza los eventos de interés y las alertas sobre la base del análisis del contenido y los patrones de metadatos.
- **Procesamiento natural del lenguaje (NLP)** Reduce significativamente los falsos positivos a través de una aplicación práctica e inteligente del NLP, léxicos complejos para cualquier idioma y tecnología de identificación de texto que reconoce descargos de responsabilidad y texto citado en correos electrónicos enlazados.
- **Visualizaciones** Visualizaciones personalizadas específicamente desarrolladas para desbloquear la capacidad de deducción propia del analista y ofrecer un máximo contexto en relación con las actividades relevantes. Comprende rápidamente el quién, qué, cuándo y cómo de las acciones de los empleados.
- **Clasificación del contenido** Implementaciones de DLP sobrecargadas que utilizan el motor de clasificación del contenido del UEBA de Forcepoint para identificar y filtrar las comunicaciones no relevantes como correo masivo y correspondencia de terceros, entre otros.

CONTACTO
www.forcepoint.com/contact

© 2018 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas comerciales de Forcepoint. Raytheon es una marca registrada de Raytheon Company. Todas las demás marcas comerciales utilizadas en este documento son propiedad de sus respectivos dueños.
[DATASHEET_FORCEPOINT_UEBA_SECURITY_ES] 030118


FUENTES DE DATOS
MOTOR ANALÍTICO
NARRATIVA INFORMADA
COMUNICACIONES
CORREO ELECTRÓNICO
VOZ
CHAT
SEGURIDAD
RED
DISPOSITIVOS FINALES
IDENTIDAD
ENRIQUECIMIENTO
ACCESO FÍSICO
DATOS DE RR. HH.
FUENTES (FEEDS) DE TERCEROS
MODELO DE DATOS
Módulo de datos extensible para todas las fuentes estructuradas y no estructuradas
CALIFICACIÓN DE RIESGO
Calificación de riesgo de la entidad y progresión a lo largo de la cadena de riesgo cibernético
COMUNICACIONES
Análisis de comunicaciones especializado: contenido y meta-análisis
VISUALIZACIONES
Visualización del análisis conductual
1. Cambio de patrones
2. Reclamos frecuentes
3. Envío de muchos correos electrónicos por la noche
4. Impresión de archivos confidenciales