Chronicle, empresa de ciberseguridad de Google que ya tiene un año funcionando, anunció hoy su primer producto comercial, llamado Backstory, una plataforma de análisis de amenazas a nivel empresarial basada en la nube que fue diseñada para ayudar a las empresas a investigar incidentes rápidamente, detectar vulnerabilidades y buscar posibles amenazas.

Las infraestructuras de red en la mayoría de las empresas generan de forma regular grandes cantidades de datos de red y registros a diario que pueden ser útiles para determinar exactamente qué sucedió al momento de un incidente de seguridad.

Pero desafortunadamente, la mayoría de las compañías no recopilan la telemetría correcta o incluso, es prácticamente imposible para ellos retener la telemetría por más de una semana, lo que hace que los analistas no puedan ver si ocurre algún incidente de seguridad antes de eso.

Backstory resuelve este problema permitiendo a las organizaciones cargar y almacenar de forma privada sus petabytes de *«telemetría de seguridad interna»* en la plataforma de nube de Google y aprovechar el aprendizaje automático y las tecnologías de análisis de datos para monitorearlo y analizarlo de forma eficiente para detectar e investigar cualquier amenaza potencial desde un panel de control unificado.

> *«Backstory normaliza, indexa y correlaciona los datos, contra sí mismos y contra terceros y señales de amenazas curadas, para proporcionar un análisis instantáneo y un contexto con respecto a la privacidad de riesgo»,* dijo Chronicle, filial de Alphabet.

> *«Con Backstory, nuestro analista sabría, en menos de un segundo, cada dispositivo de la compañía que se comunicó con cualquiera de estos dominios o direcciones IP, siempre»*, agregó.

Al igual que las soluciones SIEM, Backstory convierte los datos de registro, como el tráfico de DNS, NetFlow, los registros de puntos finales, los registros de proxy, en información significativa, de fácil búsqueda y búsqueda para ayudar a las empresas a obtener información acerca de las amenazas y ataques digitales en sus redes, pero a escala para ofrecer una imagen más completa del panorama de amenazas.

Backstory también compara los datos con las señales de *«inteligencia de amenazas»* recopiladas de una variedad de socios y otras fuentes, como VirusTotal, Avast, Proofpoint y Carbon Black, propiedad de Alphabet.

> *«Backstory compara su actividad de red con un flujo continuo de señales de inteligencia de amenazas, curadas a partir de una variedad de fuentes, para detectar amenazas potenciales al instante»,* informó Chronicle.
>
> *«También compara continuamente cualquier información nueva con la actividad histórica de su compañía, para notificarle de cualquier acceso histórico a dominios web mal conocidos, archivos infectados con malware y otras amenazas»,* añadió.

Debido a que Chronicle desea que los clientes recopilen y carguen la mayor cantidad de datos posible, Backstory no tendrá un precio basado en el volumen de datos de los clientes, sino que Chronicle venderá las licencias según el tamaño de la compañía.

> *«Construir un sistema que pueda analizar grandes cantidades de telemetría no será útil si se le penaliza por cargar toda esa información. Con demasiada frecuencia, los proveedores cobran a los clientes según la cantidad de información que procesan»,* explicó Chronicle.
>
> *«Dado que la mayoría de las organizaciones generan más datos cada año, sus*

> *facturas de seguridad siguen aumentando, pero no son más seguras»*, agregó.

Microsoft anunció recientemente servicios similares sobre análisis de seguridad, llamados Threat Hunter y Azure Sentinel, que la compañía está lanzando como el *«primer SIEM nativo dentro de una plataforma de nube importante»* para ayudar a las empresas a detectar, prevenir y responder a las amenazas en sus redes.

Splunk, una compañía que ofrece un producto similar, registró una caída de 5% en sus acciones al momento del cierre el lunes siguiente al anuncio del servicio Backstory.